



**University of Piraeus Department of Digital Systems
Post graduate program in Digital Systems Security**

Supervisor: Dr. Christos Xenakis, Lecturer

Course Student: Malissovas Achilleas – Lakis, MTE/0916

Thesis subject: Malicious programs in P2P networks

Description: Study, analysis, and evaluation of malware in networks with peer nodes. Locate executable software in P2P networks and analyze their behavior in a protected environment. Study recorded rates of malicious software on P2P networks.

Piraeus, July 2011



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

**ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΡΟΓΡΑΜΜΑ
ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ
ΔΙΟΙΚΗΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΚΑΤΕΥΘΥΝΣΗ: ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ**

ΕΠΙΒΛΕΠΩΝ: Λέκτορας Χρήστος Ξενάκης

ΜΕΤΑΠΤΥΧΙΑΚΟΣ ΦΟΙΤΗΤΗΣ: Μαλισιώβας Αχιλλέας Λάκης, ΜΤΕ/0916

**Θέμα διπλωματικής Εργασίας: Κακόβουλο λογισμικό
σε δίκτυα P2P**

Σύντομη Περιγραφή: Μελέτη, ανάλυση και αξιολόγηση κακόβουλο λογισμικού σε δίκτυα ομότιμων κόμβων. Εντοπισμός εκτελέσιμου λογισμικού σε δίκτυα p2p και ανάλυση της συμπεριφοράς τους σε ένα προστατευμένο περιβάλλον. Καταγραφή των ποσοστών κακόβουλο λογισμικού σε δίκτυα P2P και μελέτη αυτών.

Πειραιάς, Ιούλιος 2011

Περίληψη

Διάφορα είδη p2p έχουν εφευρεθεί. Κάθε τύπος δικτύου χρησιμοποιείται για το διαμοιρασμό αρχείων, με τη χρήση μιας κεντρικής οντότητας να ελέγχει το δίκτυο, ή χωρίς τη παρουσία αυτής. Την έλλειψη τέτοιας κεντρικής οντότητας εκμεταλλεύτηκαν χρήστες που διέδωσαν κακόβουλο λογισμικό για προσωπικά οφέλη. Ένας τρόπος άμυνας είναι η διαχείριση της φήμης, όπου δείκτες φήμης ορίζονται από τα άτομα που κατεβάζουν αρχεία από διάφορους ιστότοπους με torrents. Κάθε συμπεριφορά κακόβουλου προγράμματος διαφέρει από πρόγραμμα σε πρόγραμμα, αλλά για να ανοίγουν πόρτες σε ένα σύστημα για απόκτηση απομακρυσμένης πρόσβασης και άλλα για να κάνουν ζημιά σε προσωπικούς υπολογιστές. Εταιρίες που ασχολούνται με θέματα ασφάλειας, προκειμένου να ενημερώσουν τους χρήστες για τις επιπτώσεις των κακόβουλων λογισμικών, δημιούργησαν μεθόδους αξιολόγησης της ζημιάς που μπορούν να επιφέρουν και ενημέρωσης του κοινού για διάφορες απειλές όπου δεν έχει βρεθεί λύση. Για την ανάλυση της κακόβουλης συμπεριφοράς διάφορες εμπλεκόμενες εταιρίες έχουν φτιάξει οδηγίες για τη δημιουργία ενός προστατευμένου περιβάλλοντος. Τα περισσότερα από αυτά εμπεριέχουν τη δημιουργία εικονικού περιβάλλοντος και χρησιμοποιώντας συγκεκριμένα εργαλεία για τη ανίχνευση τους. Εκτός από τα εργαλεία, είναι κρίσιμο να προσεχθούν πτυχές, όπως τα χαρακτηριστικά ενός torrent, για παράδειγμα μέγεθος αρχείου και τύπος αρχείου πριν την έναρξη του διαμοιρασμού. Λαμβάνοντας αυτές τις πτυχές υπόψη, μπορεί να ανιχνευθεί κακόβουλο λογισμικό σε δίκτυο ομότιμων κόμβων.

Table of Contents

Acknowledgement.....	1
Abstract.....	2
1. Defining Peer-to-Peer networks.....	2
2. P2P Network Centralization Architecture.....	2
3. P2P Network Structure.....	5
4. Defining Malicious Software.....	5
5. Challenges in facing malicious software in p2p systems.....	6
6. Types of malware detected in p2p networks.....	7
7. Definitions of detected malware.....	7
8. Behavioral examples of previously detected malware in p2p.....	10
9. Evaluating malware threat level.....	14
10. Defining a Secure Testing Environment.....	16
11. Selecting an Antivirus.....	20
12. Percent of malware in networks and peer 2 peer.....	22
12.1. Internet Traffic and Pirated content.....	22
12.2. Malware statistics in other networks.....	26
12.3. Malware statistics in p2p.....	33
13. Searching for malware in IsoHunt.....	35
13.1. Malware found in isoHunt.....	39
14. Comparing findings with previous research.....	42
15. Conclusion.....	43
16. References.....	44
17. Figures.....	49

Acknowledgement

Finishing my MSc in Digital Systems Security, I would like to thank my mother, Konstandinia, and my sister, Katie, for their psychosocial support thought the course. I also thank all my course professors for giving me the necessary guidance and knowledge concerning security issues on the field of informatics. I would also like to thank professors Dr. Christos Xenakis and Dr. Christoforos Ntantogian for helping me in shaping the contents of the present work.

Abstract

Various types of peer to peer (p2p) networks have developed. Each network type is used to effectively transfer files, with the use of a central entity monitoring the network or without the use of such an entity. The absence of such a central entity has been exploited by users who intend to spread malware for personal gain. One way of defense is trust management, in which reputation ratings are given by users on torrent search engine sites. Various researchers have identified various types of malware propagated through decentralized p2p networks. Each malware detected has a behavior that varies from program to program, others used for opening ports on a system to enable remote access or even cause damage to personal computers. In order to inform users for the severity of malware, antivirus vendors have created methods for evaluating a malware's damage and informing the public for various new threats for which remedy is not given yet. In order to investigate malware behavior, various institutions and companies have created guidelines in creating a safe testing environment. Most of them include creating a virtual environment and using appropriate tools for malware detection. Apart from tools, it is crucial to pay attention to other aspects, concerning the characteristics of a torrent, such as file size and type before downloading.

Keywords: peer to peer networks, secure environment, malware, threat level, antivirus, malware statistics, internet traffic, BitTorrent, isoHunt.

1. Defining Peer-to-Peer networks

Rüdiger Schollmeier [1], as cited at the Proceedings of the First International Conference on Peer-to-Peer Computing in 2001, defined a Peer-to-Peer network (P-to-P, P2P,...) as a distributed network architecture where the participants (known as peers) share a part of their hardware resources, such as processing power, storage capacity, network link capacity, etc. The network utilizes these shared resources to provide its services such as file sharing or shared workspaces for collaboration. Other peers have direct access on them. The peers of such a network are simultaneously resource providers and resource requestors.

The definition made by [2] added to the upper definition, the self organization of the peers (referred as nodes) into network topologies as well as network adaptability to failures, transient nodes and the absence of a global centralized server or authority.

2. P2P Network Centralization Architecture

P2P networks are described as “overlay” networks, because the network is formed on top of the existing computer network.

Rüdiger Schollmeier [1] defined two distinguishable types of P2P networks. The first, named “**Pure**”, is the one which complies with the upper definition. Also, if a single

entity is removed at random from the network, the network will keep providing its services without loss of services. The second type of distributed P2P network architecture is named “**Hybrid**”. This type complies with the upper definition of P2P distributed networks and a central entity provides part of the network services. The difference between the two types is that in “Pure”, no central entity exists, while in “Hybrid”, a central entity is always included.

Androutsellis S. T. & Spinellis D. [2] in 2004 extended the upper identified types by including the “**Partially**” Centralized Architecture, referring to the above, “Pure” and “Hybrid”, as decentralized architectures. In the “**Partial**” type, some peers act as local sharing indexes for files shared by local peers. If a peer fails to function, the network will dynamically assign a new peer for the task, thus not providing a single point of failure. “**Hybrid**” is further mentioned by [2] (as cited by HC Kim in “P2P overview”, Technical report, Korea Advanced Institute of Technology, August 2001) as the central entity that stores the description of files shared by other peers.

Summing up, three overlay network architectures types are identified: “**Pure**”, “**Hybrid**” and “**Partial**” and are shown by the following figures.

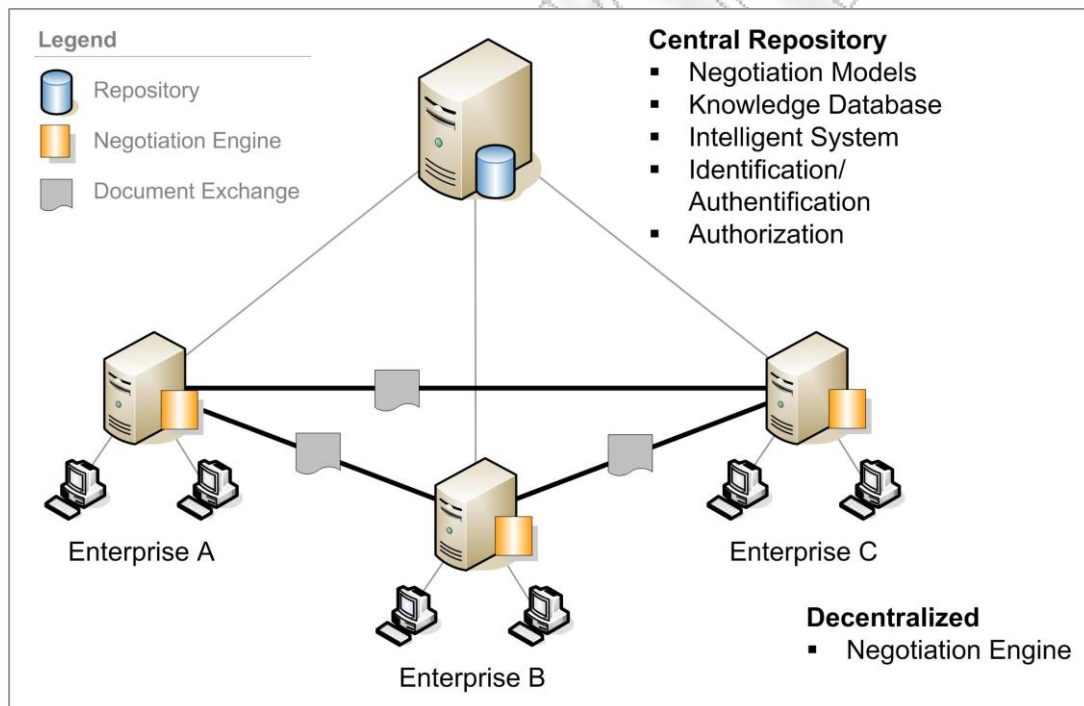


Figure 2.1: Hybrid p2p architecture [1]

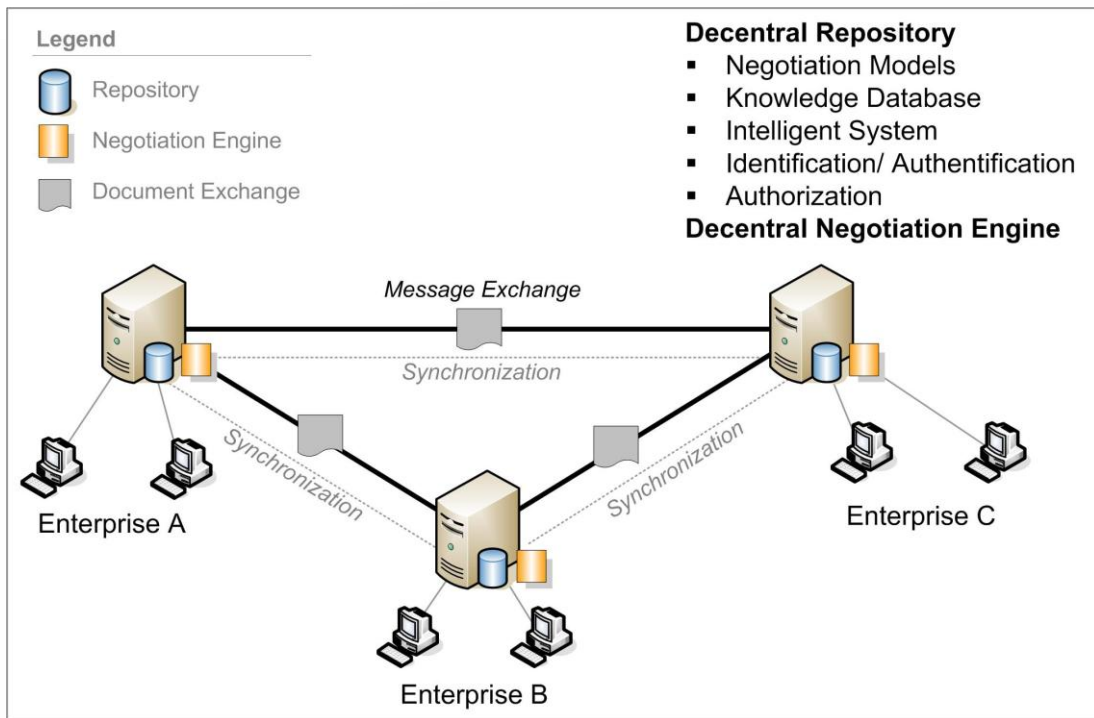


Figure 2.2: Pure p2p architecture [2]

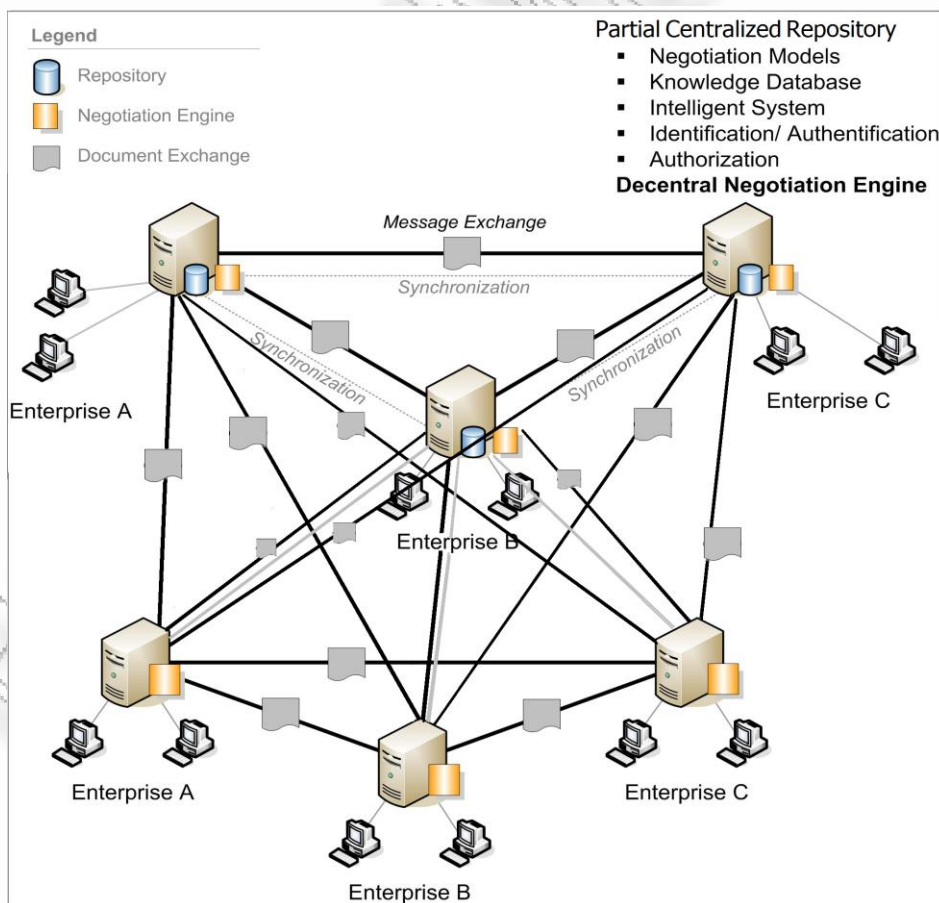


Figure 2.3: Partially centralized p2p architecture.

3. P2P Network Structure

Androutsellis S. T. & Spinellis D. [2] refer to the network structure as whether a p2p network is created without previously defined methods, by adding peers and content, or by following specific rules. Three categories defined are **unstructured**, **structured** and **loosely structured**.

Unstructured is a p2p network where the content is located by search methods such as flooding the network with queries or random peer discovery. The content placement in the network is not related to its topology. Implications in the searching mechanisms employed include availability, persistence and scalability. Unstructured networks are appropriate for highly transient peers.

Structured is a p2p network where the content is located by a type of distributed routing table, where queries discover the desired content by detecting both location of content and content as well. The content placement in the network is directly bound with the network's topology and are placed (or pointers indicating their placement) at specific locations. Structured networks are not appropriate for highly transient peers.

Loosely Structured is a p2p network between unstructured and structured. The content's location is not specified and is affected by routing hits.

4. Defining Malicious Software

A general definition of malware (malicious software) is given by Kramer S. and Bradfield C.J. [3]. The definition is formulated abstractly using a certain language of modal logic (a type of formal logic), so it can be applied to all instances of malware.

“A software system s is malware by definition if and only if s damages non-damaging software systems (the civil population so to say) or software systems that damage malware (the anti-terror force so to say).”

Damage refers to a software system causing incorrect behavior to another software system. The term “correct” refers to all the explicit possible intended states of a properly functioning software system.

A general classification of objects detected by Kaspersky Lab is published at <http://www.securelist.com/> and divides malware in two subcategories, *Malicious Programs* and *Adware, Pornware and Riskware*.

Malicious programs

Viruses and Worms

- Net-Worm
- Email-Worm
- Worm
- P2P-Worm
- IM-Worm
- IRC-Worm
- Virus

Trojan programs

- Backdoor
- Trojan
- Trojan-ArcBomb
- Trojan-Downloader
- Trojan-Dropper
- Trojan-PSW
- Trojan-DDoS
- Trojan-Spy
- Trojan-Ransom
- Trojan-Notifier
- Trojan-Proxy
- Trojan-GameThief
- Trojan-IM
- Trojan-Banker
- Trojan-Malifinder
- Trojan-SMS
- Trojan-Clicker
- Rootkit
- Exploit

Suspicious packers

- MultiPacked
- SuspiciousPacker
- RarePacker

Malicious tools

- Constructor
- DoS
- Spoofer
- Hoax
- SMS-Fooder
- Email-Flooder
- IM-Flooder
- Flooder
- VirTool
- HackTool

Adware, Pornware and Riskware

RiskWare

- Client-IRC
- Client-P2P
- Client-SMTP
- Dialer
- Downloader
- FraudTool
- Monitor
- PSWTool
- Server-FTP
- Server-Proxy
- Server-Telnet
- Server-Web
- WebToolbar
- NetTool
- RiskTool
- RemoteAdmin

PornWare

- Porn-Downloader
- Porn-Dialer
- Porn-Tool

Adware

5. Challenges in facing malicious software in p2p systems

Peer to peer systems are used among users (known as peers) to upload and download various files. Some of these file sharing protocols, like BitTorrent, allow the user to simultaneously upload and download files. This opens a channel among users for uploading files from their computers. The Government of the Hong Kong special Administrative Region [4] has listed potential security risks when exchanging files with p2p protocols.

1. Open TCP ports

A Firewall is needed to open specific ports to allow a p2p program to function properly. Those open ports may be used by attackers to transfer their malware code to the host's computer.

2. Malware Propagation

An example of malware propagation is VBS.Gnutella, a worm that propagated through the Gnutella network, and shared itself through that network. A trojan may be propagated and used for opening ports, creating backdoors.

3. Risks of downloaded content

The creator of the downloaded files is possibly unknown or untrustworthy to the user. Furthermore, the downloaded content may be illegal, exposing the

user to criminal litigation. Moreover, the source of the distributed content is untrustworthy because the user cannot figure out at any time what peers are connected and if these peers are trustworthy.

4. Vulnerability in p2p software

As any software, so does p2p software contains vulnerabilities. These vulnerabilities can be exploited in various ways, such as spread viruses, make backdoors and make denial of service attacks.

6. Types of malware detected in p2p networks

Previous research in p2p networks [5, 6, 7] focused on detecting malicious software in Gnutella, Limewire, OpenFT and BitTorrent p2p networks. Gnutella is defined as pure, according to its network architecture type and unstructured in content location [8]. The version of Limewire used in [6] is a Gnutella implementation, with pure network architecture and the network is loosely structured because some nodes (named ultrapeers) hide other nodes (named leafs) to lessen network traffic during the routing of queries, concealing indirectly the content's location from the leafs. The OpenFT as described in [6] has hybrid network architecture and a structured content location. BitTorrent [7] has pure network architecture and unstructured content distribution in the network.

Collectively, the common types of malware detected in the above p2p networks are:

1. Computer viruses
2. Worms
3. Trojans
4. Trojan-downloaders
5. Trojan-backdoors
6. Adware, dialers
7. Keyloggers
8. Exploits of Microsoft software vulnerabilities
9. Other malware types

Definitions for the above identified malware types, as well as examples for each malware type are given below.

7. Definitions of detected malware

Computer Virus: Informally defined by Cohen F. at [9], a computer virus is a program that may modify other programs, so as to include a copy of itself (or an evolved copy of itself). The capability of program modification makes every infected program to act as a virus. A virus may use the authorizations of each user in a computer system or network in order to modify other programs.

V: = [F = RANDOM-FILE-NAME; COPY V TO F;]

The above pseudo-code example provided by Cohen F.B. [10], means that a virus (V) selects a random file (F) and copies itself to F.

Worm: The pseudo-code example provided by Cohen F.B. [10] bellow, defines informally a worm.

W: = [F = RANDOM-FILE-NAME; COPY W TO F; RUN F;]

This means that a worm (W) not only copies itself in a file (F), but it executes the file it infested as well.

Trojan: A trojan/trojan horse is a malware that masquerades as an application or file. For instance, it can be a fake video file downloaded by a p2p program. When the application is executed, the trojan may contain malware, viruses or open a backdoor, infecting the computer [11]. The contents of the trojan are referred to as payload or package [11]. The payload (the malicious program) is executed when the program that carries it is being executed as well.

Trojan-Downloader: A Downloader is a trojan subcategory [12] that downloads and installs new versions of malware, such as trojans and AdWare, on computers. When the Downloader is downloaded from the Internet, the programs included are either executed or included on a list of programs to be executed at the start of the operating system.

The Downloader's code either contains information about the names and locations of the programs downloaded, or downloads such information from an Internet resource (such as a web page).

The Downloader is mostly used to initially infect users accessing websites which contain exploits.

Trojan-Backdoor: A backdoor is classified by Kaspersky's SECURELIST as a trojan subcategory [12]. A computer infected by a backdoor allows remote control by malicious users. A backdoor is similar to an administrative system. The malicious user can use the infected computer to execute various tasks, such as delete files and execute programs. Backdoors are often used to create a zombie or botnet network, a unified group of infected computers, which are under the command of the malicious user and utilized for illegal purposes.

Trojan-Adware: Adware [13] are programs used to enhance advertisement, such as displaying advertisements, collecting sites the user visits or redirecting the user to the advertiser's site. Adware may be installed onto a user's computer by 1) freeware (adware is built-in) or 2) by visiting an infected website. The adware aims for product registration or payment in order to stop its functioning. The data usually collected by the adware are: 1) computer's IP address, 2) operating system and browser version, 3) frequently visited sites 4) search queries, 5) other data utilized for advertisements. The

trojan-adware does not notify the user for gathering information and it is classified as malware. If the adware informs the user for gather information, then it is not considered as a malware.

Dialer: A dialer is a subcategory of Riskware, legitimate programs that may cause damage if they are used by malicious users [14]. This program creates telephone connections through a modem. If the dialer was not installed by the user or the system administrator, then it may pose a threat, such as downloading information from a web site by exploiting program vulnerabilities.

Keylogger: A keylogger (keystroke logger) intercepts key presses in order to obtain confidential data [15]. They are usually deployed by trojan backdoors that relay the intercepted data to malicious users for illegal and unauthorized purposes.

Exploit software vulnerabilities: The web site of Securelist [16] mentions that a software system's vulnerability refers to software states where a weak security rule or a problem within the software is exploited. The seriousness of their weakness depends on whether such vulnerabilities are used to cause damage to the computer system or not.

The Common Vulnerabilities and Exposures dictionary (CVE), developed by the MITRE Corporation that is co-sponsored by the National Cyber Security Division of the U.S. Department of Homeland Security, developed the terms "vulnerability" and "exposure" regarding information security as follows:

Vulnerability: Vulnerability is a mistake in software where a malicious user may take advantage of it to gain access to a network or a system. Vulnerability is also considered "*a state in a computing system (or set of systems) that either:*

- *allows an attacker to execute commands as another user*
- *allows an attacker to access data that is contrary to the specified access restrictions for that data*
- *allows an attacker to pose as another entity*
- *allows an attacker to conduct a denial of service"*

The CVE has made a vulnerability list at: <http://www.cve.mitre.org/cve/index.html>. Some of them are:

- *phf (remote command execution as user "nobody")*
- *rpc.ttdbserverd (remote command execution as root)*
- *world-writable password file (modification of system-critical data)*
- *default password (remote command execution or other access)*
- *denial of service problems that allow an attacker to cause a Blue Screen of Death*
- *smurf (denial of service by flooding a network)*

Exposure: Exposure is a system configuration issue or a mistake in software that may indirectly compromise a system or network and violating a security policy. An "exposure" is a state that:

- allows an attacker to conduct information gathering activities
- allows an attacker to hide activities
- includes a capability that behaves as expected, but can be easily compromised
- is a primary point of entry that an attacker may attempt to use to gain access to the system or data
- is considered a problem according to some reasonable security policy

The CVE has made a vulnerability list at: <http://cve.mitre.org/>. Some of them are:

- running services such as finger (useful for information gathering, though it works as advertised)
- inappropriate settings for Windows NT auditing policies (where "inappropriate" is enterprise-specific)
- running services that are common attack points (e.g., HTTP, FTP, or SMTP)
- use of applications or services that can be successfully attacked by brute force methods (e.g., use of trivially broken encryption, or a small key space)

8. Behavioral examples of previously detected malware in p2p

The following examples come from the malware detected by [5, 6 and 7] during their research for malicious software in p2p systems. Though some types, such as keyloggers, are detected during their research, no specific name of such detected software is given in their research so as to present a specific malware here. The behavior of the following malware comes from reports by companies providing security product solutions and other software providers.

Trojan.Downloader.Istbar-176 (classified by ClamAV)

An example of a Trojan-Downloader is *Trojan.Downloader.Istbar-176* (as classified by ClamAV). *Istbar* means Internet Site bar, meaning that this trojan utilizes site bars to achieve its malicious purpose. An alias of it in Kaspersky Labs is *Trojan-Downloader.Win32.IstBar.us* and it has various versions and aliases. One such alias is named *Trojan-Downloader.Win32.Small.cdk* [17].

Trojan-Downloader.Win32.Small.cdk is a windows PE executable file and its size is approximately 6KB. It is compressed by NsPack, software that compresses executable files which the system may execute without the need to decompress them [18]. The decompressed file is approximately 32KB and written in C++.

When the trojan is launched, a registry key is created, flagging its repeated launch:

```
[HKCU\Software\Microsoft\Windows\CurrentVersion]
"adv470" = "adv470"
```

The numbers "470" in the parameter differ in each trojan version.

In order to achieve unrestricted access to the Internet, this trojan locates firewall (for instance, Agnitum Outpost, ZoneAlarm, and Windows XP SP2 firewall) activity. Then, it searches for windows which ask the user whether to block such activity, so as to cause the permission of its activities.

For example, the trojan will search for an Agnitum Outpost window with the following heading:

"Create rule for <name of current file>"
"Warning: Components Have Changed"
"Hidden Process Requests Network Access"

Then the trojan ticks the box marked "Allow all activities for this application" and presses "OK".

The trojan also downloads and executes the files listed below on the victim machine:

- http://iframeurl.biz/***/dl.php?adv=adv470 — will be saved as %Windir%\uniq;
- http://iframeurl.biz/***/kl.txt — will be saved as %Windir%\kl.exe;
- http://iframeurl.biz/***/tool2.txt — will be saved as %Windir%\tool2.exe;
- http://iframeurl.biz/***/country.php — will be saved as %Windir%\country.exe;
- http://iframeurl.biz/***/secure32.php — will be saved as %Windir%\secure32.html;
- http://iframeurl.biz/***/paytime.txt — will be saved as %System%\paytime.exe;
- http://iframeurl.biz/***/hosts.txt — will be saved as %Windir%\hosts;
- http://iframeurl.biz/***/dluniq..... — will be saved as %Windir%\uniq.

The trojan will download the following file to Italian versions of the operating system:

- http://iframeurl.biz/***/it.txt — will be saved as "%Windir%\countrydial.exe"

The trojan will download the following files to non-Italian versions of the operating system, and launch them for execution:

- http://iframeurl.biz/***/tool1.txt — will be saved as %Windir%\tool1.exe;
- http://iframeurl.biz/***/tool3.txt — will be saved as %Windir%\tool3.exe;
- http://iframeurl.biz/***/tool4.txt — will be saved as %Windir%\tool4.exe;
- http://iframeurl.biz/***/tool5.txt — will be saved as %Windir%\tool5.exe;
- http://iframeurl.biz/***/ms1.php — will be saved as %Windir%\ms1.exe.

BackDoor-AZV

An example of a Trojan-Backdoor is *BackDoor-AZV*, as mentioned by Dmitry Gryaznov in [5] and located it at Usenet. The *BackDoor-AZV*, according to McAfee

Labs, is used to access remotely a computer system. The trojan camouflaged itself as an attached article, photo, icon or a zipped file with the .exe extension on an e-mail. There are multiple versions of this trojan, most of which aim on connecting to an Internet Relay Chat (IRC) server on port 6666 or 6667 and let the attacker execute orders from the infected PC, such as: download remote file, act as socks4 proxy, terminate process and read IRC log file. The recent version of this trojan tries to download a worm named *W32/Brepibot* from four different sites. When the worm is run, it copies itself to the Windows System directory, for example, c:\Windows\System32\csrnvrt.exe. Then, the following registry key is created to load the worm at startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "WindowsDiskLog" = csrnvrt.exe
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "WindowsDiskLog" = csrnvrt.exe

The worm when executed may 1) contact a list of remote IRC servers and 2) wait for further instructions. The attacker may receive information about 1) the infected system's uptime and 2) execute or delete files [19].

Downloader-UA.h (installs adware named FbrowsingAdvisor and SurfingEnhancer)

An example of a trojan installing adware is *Downloader-UA.h*. It disguises itself as fake music (mp3) or video (mpg) files which are associated with fastmp3player.com [20]. All of the infected sample files listed at [20] contain the "t-3545425-" characters in their name. When the user executes the fake file, she is directed to download a file named PLAY_MP3.exe and does not listen or view the expected file's content.

If the user agrees to download and run PLAY_MP3.exe a 4,800 word EULA is displayed.



As stated by Schmugar, C. at McAfee Labs [42] the EULA contains inaccurate statements such as:

(3) *The Licensed Materials you install will also include/be bundled with the following 3rd Party software products:*

PRODUCT Mirar AND EULA <http://policy.getmirar.com/>

and

22. Effective: January 14, 2007.

END OF DOCUMENT

NetNucleus Privacy Policy/EULA

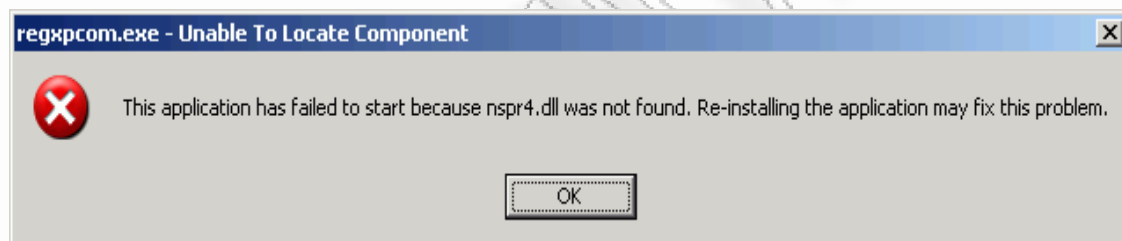
This End User License Agreement (the "Agreement") is a legal agreement between you and NetNucleus Corp.

indicating an integrity violation of the EULA as well as suspicious behavior of the components to be installed.

When the user selects "I agree" to the EULA, adware "FBrowsingAdvisor" and "SurfingEnhancer" is installed as described in the EULA. Schmügar also mentions the directory that PLAY_MP3.exe will create:

c:\Documents and Settings\tani\My Documents\Dreamsoft\Firefox\firefox_adware\FF-Source\Source\Release\XPCOMEvents.pdb

If the user has not installed Firefox she may see the following error message:



FbrowsingAdvisor is an adware that, when installed on the user's PC displays a large number of popup and pop-under advertisements [21] based on user preferences and search history. The information derived from the user's web preferences is transmitted. *SurfingEnhancer* is an adware similar to *FbrowsingAdvisor* that collects the user's web preferences and compares them with other user preferences so as to provide customized recommendations to registered users.

Summing up, PLAY_MP3.exe from PlayMP3.biz is a browser control masquerading as an executable file, does not play the user's MP3 files, and after the adware installation, floods the user with unwanted advertisements.

Exploit-MS04-028(software vulnerability)

An example of software vulnerability is *Exploit-MS04-028*. Gryaznof detected JPEG files exploiting the vulnerability of MS04-028 in Gnutella in 2005[5]. In JPEG processing (GDI+), a buffer overrun could occur, allowing code to be executed automatically when the images are viewed [22]. The software vulnerability concerned Microsoft Windows XP, Service Packs 1, 2 and 3, as well as a wide range of Microsoft product software, such as Microsoft Office XP, Microsoft Visual Studio.Net 2003 and Microsoft Digital Image Pro version 9.

9. Evaluating malware threat level

A specific evaluation level for malware in p2p does not exist. In general, various security organizations have developed similar methods in 1) determining the threat level of each malware and 2) reflect changes in malicious traffic and the possibility of disrupted connectivity over the Internet. An example for determining the threat level of each malware comes from Panda security and an example for global changes in malware traffic come from SANS's Internet Storm Center "infocon".

Panda security [23], a security products firm, defines four security threat levels. Every malware detected is assigned one threat level to inform users of the possible risks faced. The threat level is dependent on: 1) its distribution and 2) the damage it can cause.

The table below illustrates the threat level based on the damage it causes and its distribution. The y-axis represents the 'Damage level' with categories 'Severe' and 'High'. The x-axis represents the 'Distribution' with categories 'Not widespread', 'Moderately widespread', 'Very widespread', and 'Epidemic'. The threat levels are color-coded: Low (white), Moderate (light red), High (medium red), and Severe (dark red).

Damage level	Distribution			
	Not widespread	Moderately widespread	Very widespread	Epidemic
Severe	MODERATE threat	HIGH threat	SEVERE threat	
High	LOW threat	MODERATE threat	HIGH threat	SEVERE threat

Figure 9.1: Threat level table [3].

The above figure is explained as following:

- **Low threat:** malware is neither damaging nor widely spread.
- **Moderate threat:** malware is either fairly widely spread and causes significant damage or not widely spread but causes serious damage.
- **High threat:** malware is either very widespread and causes damage or relatively widespread and seriously damaging.
- **Severe threat:** malware is widely spread and very damaging.

Logically, the threat level of a malware can vary, from low threat in one moment to severe in another, depending on how widespread it becomes. The Panda Threat Level monitors these changes in real-time.

Distribution refers to the spread of a malware. The more widespread a malware is, the higher the probability it has to infect user computers.

The infection rate determines the malware distribution. The rate measures the percentage of infected computers against the total number of computers scanned.

The damage levels of a malware are:

- **Epidemic:** the percentage of computers examined and infected by the malware is alarming.
- **Very widespread:** The percentage of computers examined and infected by the malware is more than 3%.
- **Moderately widespread:** The percentage of computers examined and infected by the malware is more than 1.0% and less than 3%.
- **Not widespread:** Less than 1.0% of computers are infected by the malware.

The Damage level refers to the possible damage a malware can cause in a computer. This damage can be more or less severe: messages appearing on the screen, lost or altered information, collapsed systems, program malfunctions, etc.

The damage levels of a malware are:

- **Severe:** causing serious damage. For example, the destruction or modification of files, formatting hard drives, sending information to third parties, generation of heavy traffic in servers, reducing system performance, opening security holes, permanent damage, etc.
- **High:** causes moderate effects. All malware, as inoffensive as they may seem, attempt to cause damage to the user. Those that do not result in destructive action are classified as simply moderately damaging. For example, those creating messages to appear on the screen.

The Panda Virus Laboratory establishes the level of damage when the malware in question is analyzed for the first time.

“INFOCon” [24] is a qualitative approach in depicting changes in malicious traffic and possible network disruption. The concept of “Change” in traffic caused by malware propagation through hosts is what “INFOCon” is all about. When the malware is detected and the number of infected machines does not increase, then the traffic is unlikely to cause disruptions.

Five INFOCon definitions exist:










 infocon: GREEN  http://isc.sans.org	Everything is normal. No significant new threat known.
 infocon: TEST  http://isc.sans.org	This status is used for testing only. Everything is normal. No significant new threat known.
 infocon: YELLOW  http://isc.sans.org	We are currently tracking a significant new threat. The impact is either unknown or expected to be minor to the infrastructure. However, local impact could be significant. Users are advised to take immediate specific action to contain the impact. Example: 'MSBlaster' worm outbreak.
 infocon: ORANGE  http://isc.sans.org	A major disruption in connectivity is imminent or in progress. Examples: Code Red on its return, and SQL Slammer worm during its first half day
 infocon: RED  http://isc.sans.org	Loss of connectivity across a large part of the internet.

Figure 9.2: INFOCon definitions [4]

10. Defining a Secure Testing Environment

Creating an environment that mitigates the impact of computer and network infection, detecting malicious behavior as well as eliminating threats due to software vulnerabilities or system exposures is dealt with by various researchers and IT security companies [25], [26], [27],[28], [29], [30]. Previous researchers checking peer to peer systems for malicious content took precautions such as using a virtual machine and an antivirus. Specifically, Berns, D.A. and Jung, E. [7] downloaded the metainfo file of the designated torrents. Then, they transferred the metainfo files on a virtual machine and downloaded the actual files from that virtual machine. An antivirus software package, ClamAV, was used to check for malicious programs. Kalafut, A., Acharya, A. and Gupta, M. [6] mentioned using only ClamAV for scanning malware. Fahimian, S. et al [31] proposed detection of passive worms in peer to peer networks by relating hash value with files.

Previous publications in creating a secure computer system laboratory point out various countermeasures. For example, Aycock, J. and Barker, K. from the University of Calgary, Canada [25], created a laboratory for the course on computer viruses and malware, considering five security aspects: *legal, ethical, social, behavioral, and technical*. Legal safeguards include 1) teaching students the legal repercussions of malware creation and release, and 2) imposing contractual legal obligations on the students. The ethical aspect included 1) ethical theories, decision making and moral development and 2) ethics for computer professionals and the AVIEN and EICAR principles of conduct. The social aspect covers social pressure among peers by 1) working in teams, 2) by making a machine accessible only when all users of a designated team have logged in and 3) reminding students the laboratory protocol that they are jointly accounted for actions taken in the lab. This approach is justified in order to 1) avert collusion among students and 2) evade accidental bypass of security

safeguards. Behavioral safeguards regulate conduct in the laboratory, including a laboratory protocol created by taking into account biohazard protocols and antivirus researchers. The protocol is associated with the technical safeguards. Technical safeguards include 1) physical security of the laboratory and its machines and 2) electronic security. Specifically, physical security included:

- a key card lock
- brick walled access area with one door and no windows
- door closer and alarm when opened to long
- disabled and physically disconnected network ports
- two motion-triggered ceiling cameras and ZoneMinder to manage camera output
- specified areas (using bright colored tape named 'media line') restricting outside electronic devices and media
- bookcase to leave restricted items in the laboratory, not passing the media line

Other equipment includes:

- Sun Blade 100 server with RAID disks running Solaris, Samba and rsync servers
- network switch connecting the server with other lab machines (ports locked to MAC address of lab machines)
- Student machines had the following:
 - 1.4GHz P4 Xeons
 - at least 256Mbyte RAM and at least 10Gbyte hard drive
 - Red Hat Linux 9
 - VMware Workstation
 - FreeBSD 4.9 on VMware
 - Red Hat set to run only VMware on login

Input/Output security of machinery included

- PS/2 (not USB) keyboard and mouse
- video monitor
- network
- read-only CD-ROM drive
- I/O ports on motherboards disabled from BIOS
- lock down various BIOS settings (enable BIOS password and chassis intrusion detection)
- Padlocking lab machines to their associated tables

It also states phases for commissioning, operation and decommissioning of the security laboratory.

Hu, J., Cordel, D. & Meinel, C. in [27] proposed an online virtual laboratory for IT security education. Their research focuses on technical issues rather than ethical or social. Their approach is an advancement of their Tele-Lab "IT-Security", where the use of virtual machines substitutes physical machinery, as well as making the laboratory mobile for the user and accessible though the internet. The user will log on

the host from a web browser and a virtual machine with open-source security tools is assigned to the user. Their purpose for adopting virtual machines is to:

- allow users to experiment with an operating system with full administrator privileges
- avoid the user's direct exposure of underlying computing hardware and software infrastructure by restricting malicious behavior and vulnerabilities on virtual operating systems
- reduce cost for creating a laboratory
- ease of access through the internet

The architecture of the system is divided in three units. The user unit runs a browser and an applet. The control center (run on the host) consists of a virtual machine monitor, a virtual machine manager and a user monitor. The third unit (run on the host) consists of target servers that run virtual machines and the user machine pool that contains the virtual machines allocated to the users. Specifically, client and server have the following components:

Client:

- web browser which supports Java virtual machine
- TightVNC - a remote desktop access made as a JAVA applet desktop viewer embedded on the user's desktop

Server:

- Linux operating system
- Apache web server equipped with Perl and PHP interpreters
- virtual machine
 - User-Mode Linux
 - open-source security tools
 - Secure SHell (SSH) server - secure access to a remote host
 - assigned IP address

It appears that emphasis is given on quick deployment of the virtual machine from the host. The user only needs to log on from the internet without needing to create a secure environment himself. Everything done is made through remote desktop gaining access on a virtual machine instead of actual machinery.

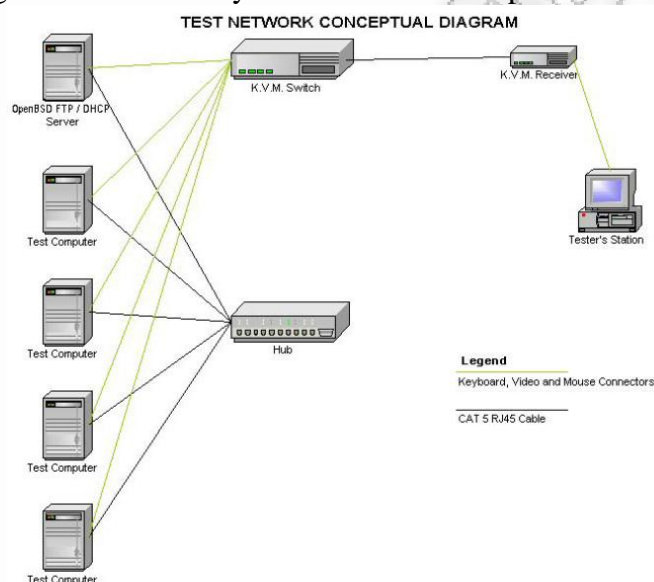
Secureops, a Canadian corporation that provides security services proposes the following solution for building a security test environment based on previous research [28]. They first state that requirements should be defined:

- Testing requirements: Take various threats into account and how they will affect security defenses and countermeasures.
- Physical security: Restrict access of computer and network components.
- Ease of access: Users should be able to manage data without real physical machinery access.
- Ease of restoration: Re-installation of operating systems within minimum time and manpower.
- Network isolation: Air-gapping and physical security address this issue.

Afterwards, hardware and software components as well as various uses of the test environment are reported. VMware is chosen because up to eight virtual machines can run simultaneously with diverse operating systems, which can form a virtual network. The drawback on this solution is that various network appliances, such as IDS sensors cannot be connected to a virtual hub and need a physical hub instead. Specifications for running five to eight virtual machines are also stated and are:

DUAL CPU 1+ GHz or (1) 2.0+ GHz
1.5 GB RAM
HD (2) 7200 RPM RAID 0 stripe
Drive Space 60+ GB

The concept diagram of the security test environment is presented below.



Considering equipment used, five computers no longer used in the company's production are used. Four of them will host VMware and one will host operating system images and testing tools, acting as a DHCP server and fileserver. A KVM switch (keyboard visual display unit, mouse) is used to control multiple computers from a single keyboard, video monitor and mouse. Hubs are also used to allow sniffers and IDS sensors. Considering operating systems, various Windows and Linux operating system images were used upon VMware for diversity and OpenBSD for the file server.

Other precautions dealt with configuration requirements. Specifically, the file server computer had its hard drive filled with zeroes using a Linux utility named "DD", while the netBSD "DD" was used on the other computers. This action provides a cleaner hard disk from "garbage" to allow forensics experimentation. Furthermore, air gap is used to isolate the test lab from the company's networks.

The restoration process involved G4U's hard disk image cloning for PC due to its free distribution, usage of FTP and ease of creating and restoring images. The report

concludes that the lab can be used for forensics testing, firewall and security appliance testing as well as virus and exploit signature research.

Taking a look at the above solutions, the common components in all three solutions is adopting virtual machines. Derived by [27], virtual machines are classified in two categories, taking into account the platform upon they are built:

- virtual machines implemented directly on the physical hardware (e.g. IBM's VM/370 VMware)
- virtual machines implemented completely on the top of a host operating system (e.g. User-Mode Linux)

The solution adopted by all the above is virtual machines running on top of operating host systems. All three publications wish to neutralize possible malicious network traffic by either:

- disabling network devices
- air gapping the virtual network from other existing networks
- running virtual machines on the host with user authentication to access them from remote desktop

The major difference is the ethical concerns stated by [25], while the other two rely more on technical solutions. Similarities are also detected with the researchers of malicious programs in peer to peer systems. For instance, Berns, D.A. and Jung, E. [7] also deployed a virtual machine for downloading untrusted code. The difference is that in research defining a secure laboratory, no testing tools for codes are mentioned, while some researchers for malware in peer to peer mention using ClamAV due to it being open sourced.

11. Selecting an Antivirus

SANS institute, a non-profit organization dealing with information security has published guidelines for choosing an antivirus [32]. First, information is given on how antivirus software works. The technologies employed in detecting viruses are:

- Signature matching – Matching the code in dispute with virus signatures from databases
- Heuristic Checksum – Matching the code in dispute with virus behavior signatures from databases
 - Static heuristic – Analyze the code for any routine or subroutine matching a virus behavior signature
 - Dynamic heuristic – The code in dispute runs into a virtual machine to analyze the behavior
- Integrity Checksum – Compare the code's checksum with the clean checksum
- Activity blocker – Blocks and alerts the user for activities done by a code

An antivirus detects a virus by scanning real-time, on-access and on-demand. It is mentioned that an antivirus cannot offer 100% protection and cannot always repair damage done by malicious software. The proposed evaluation criteria for choosing an antivirus solution are the following:

- Detection
 - Detection rate of viruses. Antivirus products are tested against two lists, where two detection rates derive: An In-The-Zoo virus detection rate and an In-The-Wild virus detection rate.
In-The-Zoo: lab viruses that have not been encountered in the real world.
In-The-Wild: viruses that have been infecting computers worldwide
A list of the In-The-Wild viruses is kept by the WildList Organization International and can be found at <http://www.wildlist.org>.
 - Circumstances under which a virus is detected (for example, detect during file download and during execution in memory)
 - Do not execute real viruses to test the antivirus solution, unless you are an antivirus expert and have taken all the necessary precautions
 - Use Eicar's (European Institute for Computer Ant-Virus Research) safe antivirus test string from www.eicar.org
 - Verify antivirus detection rates from external sources such as:
 - VB100: Provided by Virus Bulletin, VB100 is a free of charge certification for products that detect 100% of malware from the In-The-Wild virus list and no false positives are generated during the scanning of clean files [<http://www.virusbtn.com/vb100/index>].
 - AV-Test: AV-Test is an independent IT security institute that provides security oriented services, one of which is product review and certification based on the quarter of the year, the platform running (for example windows xp and windows 7), protection, repair and usability. Protection includes [<http://www.av-test.org/certifications>]
- Technology
 - Antivirus compatibility with system's hardware and software configuration
 - Scanning of all the system's areas when the virus tries to infect them (On-Access or Real-Time scanner)
 - Scanning files on user's demand
 - Ability to scan all file types
 - Use of heuristics, such as content and transmission patterns to detect unknown viruses
 - Script blocking
 - Scanning of email attachments
 - Scanning within compressed files
 - Detection of trojan, malicious active-X controls and Java applets
- Maintenance
 - Updating the virus definition library concerns:
 - Ease of update

- Frequency of released updates
 - Impact on bandwidth during the update download
 - Speed of deploying updates
 - Upgrade antivirus product software
 - Check if the older version has to be uninstalled first
 - Check when its scanning engine is upgraded
- Performance of the antivirus
 - Measure the time needed for different scans
 - Measure memory and CPU usage (using tools such as Microsoft's Reliability and Performance Monitor)
 - Check if third parties during their antivirus assessments have applied the same settings among the products, such as the same level of heuristic protection and file extension scanning
- Manageability
 - Check if management actions can be performed, such as establishing and enforcing policies, virus definition updates, view alerts, reports and logs
 - Management solution must not overburden network traffic
- Technical support
 - Levels of support according to individual needs
 - Online support, such as sending suspicious files
 - Alerts for new viruses in the wild on time
- Third party tests and reviews
- Product vulnerabilities
- Vendor profile in the antivirus market

12. Percent of malware in networks and peer 2 peer

12.1. Internet Traffic and Pirated content

Research on internet traffic has revealed the following. Envisional, an internet intelligence firm was commissioned by NBC Universal to analyze bandwidth usage across the internet to find out how much of it is used on copyright infringement. The report was published January 2011 [33]. The firm found out that 23.76% of traffic was estimated to be infringing.

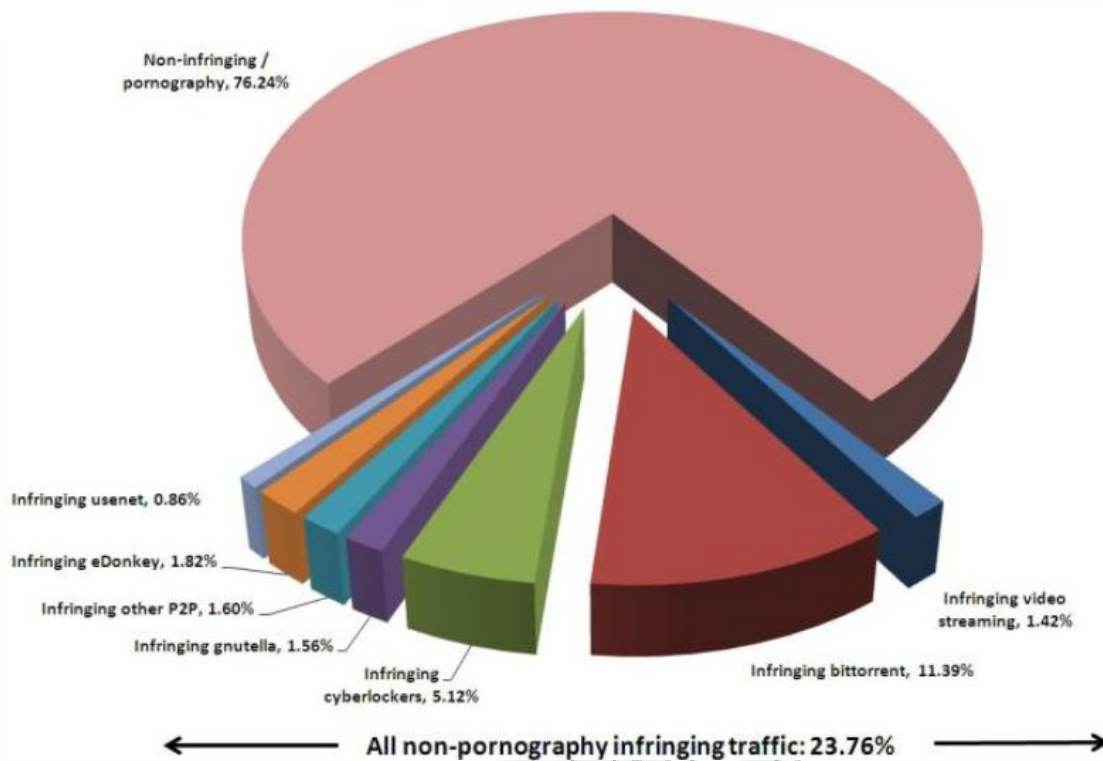


Figure 12.1.1: Estimate of infringing use of global internet bandwidth

BitTorrent traffic is estimated for 17.9% for all internet traffic. Nearly two-thirds of this traffic is estimated to be non-pornographic copyrighted content, illegitimately shared such as films, music, television episodes, software and computer games (63.7% of all bittorrent traffic or 11.4% of all internet traffic). Cyberlocker traffic is estimated to cover 7% of all internet traffic. Other p2p traffic is 5.8%. Adding up, the global traffic of p2p is 30.7%. 73.2% of non-pornographic cyberlocker site traffic is copyrighted content being downloaded illegitimately (5.1% of all internet traffic). Video streaming traffic, the fastest growing area of the internet, is estimated to account for more than one quarter of all internet traffic. Analysis estimates that while the vast majority of video streaming is legitimate, 5.3% is copyrighted content and streamed illegitimately, 1.4% of all internet traffic. The illegal content comes mostly from hosts of sites such as MegaVideo and Novamov rather than sites often used for legitimate user generated content such as YouTube and DailyMotion.

Concerning BitTorrent specifically, 2.72 million torrents managed by PublicBT, the largest BitTorrent tracker, were examined. The analysis revealed that nearly two-thirds of all content is copyrighted and shared illegitimately. Further results on the 10,000 most popular content managed by PublicBT showed that:

- 63.7% of content managed by PublicBT was non-pornographic content that was copyrighted and shared illegitimately
- 35.2% was film content – all of which was copyrighted and shared illegitimately

- 14.5% was television content – all of which was copyrighted and shared illegitimately. Of this, 1.5% of content was Japanese anime and 0.3% was sports content.
- 6.7% was PC or console games - all of which was copyrighted and shared illegitimately
- 2.9% was music content – all of which was copyrighted and shared illegitimately
- 4.2% was software – all of which was copyrighted and shared illegitimately³
- 0.2% was book (text or audio) or comic content – all of which was copyrighted and shared illegitimately
- 35.8% was pornography, the largest single category. The copyright status of this was more difficult to discern but the majority is believed to be copyrighted and most likely shared illegitimately⁴
- 0.48% (just 48 files out of 10,000) could not be identified
- one was non-copyrighted: a file containing a list of IP addresses to help users protect themselves against spam and peer to peer monitoring
- The analysis suggests that private BitTorrent sites are mostly used for illegitimate sharing of copyrighted material.
- From the following figure, the most seeded files are films (69.05%) while almost evenly, films and pornography and leeches (37.73% and 35.57% each).

Content type	Seeds			Downloaders (leechers)			Total
	Seeds in top 10,000 swarms	Percent of all seeds in top 10,000	Estimated seeds across all swarms	Downloaders in top 10,000 swarms	Percent of all downloaders in top 10,000	Estimated downloaders across all swarms	Total peers (seeds plus downloaders)
Films	3,220,293	69.05%	9,084,608	812,648	37.73%	2,404,271	11,488,879
Pornography	347,618	7.45%	980,648	766,157	35.57%	2,266,725	3,247,372
Television	538,607	11.55%	1,519,437	289,426	13.44%	856,285	2,375,723
Music	170,989	3.67%	482,369	37,399	1.74%	110,647	593,016
Software	99,645	2.14%	281,104	71,259	3.31%	210,824	491,928
PC Games	78,543	1.68%	221,574	91,059	4.23%	269,404	490,978
Console games	85,118	1.83%	240,122	44,148	2.05%	130,615	370,737
Unknown	58,687	1.26%	165,559	6,630	0.31%	19,615	185,174
Books (incl. audiobooks)	41,621	0.89%	117,415	2,777	0.13%	8,216	125,631
Anime	12,536	0.27%	35,365	24,211	1.12%	71,630	106,994
Sports	10,337	0.22%	29,161	8,046	0.37%	23,805	52,966

Figure 12.1.2: Content type, seeds and downloaders in PublicBT.

12.2. Malware statistics in other networks

Statistics exist, concerning malicious software in the internet, made by government initiatives and information security companies. In Europe, Eurostat, the statistical office in the European Union, on 8 February 2011 published a report concerning internet security. The report was made by data gathered from a survey on Information and Communication Technologies usage by households and individuals in the EU27, mostly gathered in the second quarter of 2010. Among other results concerning internet security, it reported that nearly one third of internet users (31%) in the EU27 have caught a computer virus, despite the fact that 84% of internet users use IT security software for their protection [34]. Financial loss due to “phishing”, “pharming” and or payment card misuse was 3%. The following figures show the countries with the highest and lowest rates.

Internet Security Issues	EU27
Caught a virus or other computer infection (worm, trojan horse, etc.)	31%
Abuse of personal information sent on the internet and/or other privacy violations	4%
Financial loss due to 'phishing', 'pharming' or payment card misuse	3%
Use any kind of IT security software or tool (anti-virus, anti-spam, firewall, etc.)	84%
Reported incidence of children accessing inappropriate web-sites or connecting with potentially dangerous persons	5%
Use a parental control or a web filtering software	14%

Figure 12.2.1: Internet Security issues and average ratings concerning the European Union

Caught a virus or other computer infection (worm, trojan horse, etc.) EU27 31%			
Highest		Lowest	
Bulgaria	58%	Austria	14%
Malta	50%	Ireland	15%
Slovakia	47%	Finland	20%
Hungary	46%	Germany	22%
Italy	45%		

Figure 12.2.2: Infected computers per households and individuals

Financial loss EU 3%			
Lowest		Highest	
Bulgaria	1%	Latvia	8%
Czech Rep	1%	United Kingdom	7%
Lithuania	1%	Malta	5%
Poland	1%	Austria	5%
Slovenia	1%		
Slovakia	1%		

Figure 12.2.3: Financial loss due to “phishing”, “pharming” and or payment card misuse

Any use of IT security software EU 84%			
Highest		Lowest	
Netherlands	96%	Latvia	62%
Luxembourg	91%	Romania	64%
Malta	91%	Estonia	65%
Finland	91%	Italy	67%

Figure 12.2.4: Use any kind of security software, such as antivirus, antispam and firewall

The above results depict that 84% averagely uses a way to protect itself, indicating a part of security awareness, but 31% averagely of computer users have suffered from malware. This brings up questions such as: How much time did the average individual lost due to malware infection? What sort of files did the malware damage or deleted? Does the average user know how to operate correctly a security solution to cut down malware? Would an increase in web filtering for children mitigate the average infected user? What networks does malware use to spread itself through the internet? What are the most common types of malware?

Dmitry Gryaznov, an associate of McAfee Avert, in 2005[5] stated that malware spreads itself through networks and services such as:

- Usenet – the set of people who exchange articles tagged with one or more universally-recognized labels [35]
- Internet Relay Chat (IRC)
- P2P
- Instant Messaging (IM)
- email

The following figure is Gryaznov's findings

Top ten malware detections in <u>Usenet</u> in 2005		Top ten malware detections in <u>IRC</u> in 2005		The top ten malware detections in <u>P2P (Gnutella)</u> in 2005	
BackDoor-AZV	46,963	W32/Drefir.worm	453	Downloader-TS	7,540
W32/Spybot.worm.gen.b	4,876	IRC/Flood	319	W32/Tibick!p2p	1,764
BackDoor-CQZ	1,381	VBS/Redlof@M	224	W32/Generic.d!p2p	1,597
W32/Swen@MM	283	IRC-Contact	224	W32/Sndc.worm!p2p	1,438
W32/Torvil@MM	192	VBS/Gedza	143	VBS/Gedza	1,029
MultiDropper-DC	183	Downloader-TS	107	W32/Bagle.aa@M	784
W32/Kelvir.worm.gen	75	BackDoor-JZ	71	Exploit-MS04-028	757
W32/Netsky.p@MM	75	W32/Pate.b	42	W32/Pate.b	649
BackDoor-ACH	72	W32/Jeefo	40	W32/Sdbot.Worm.gen	566
BackDoor-Sub7.svr	44	Nuke-Vai	40	W32/Bagle.n@MM	535

Figure 12.2.5: Gryaznov's findings using McAfee technology for Usenet, IRC and Gnutella

From the upper figure, the following are derived:

- From 54144 malware in Usenet, the 89,50% consists of BackDoor malware.
- From 1663 malware found in IRC, 69,45% aim to create botnets using BackDoor malware
- From 16659 malware found in Gnutella, 46,26% are trojan files in general and 40,12% (6684 files) aim in creating back doors.

From the above, the author concludes that most malware tries to create BackDoors to install malware, gaining access on the computer's files and hardware resources. Interesting are the annual reports in 2010 by Symantec, Kaspersky and McAfee, three information security technology providers.

Symantec's annual security report for 2010 [36] states that:

- Email
 - Global spam rate: 89.1%
 - Global virus rate: 1 in 284.2 (0.35%)
 - Global phish rate: 1 in 444.5 (0.22%)
 - only 0.7% of spam was sent from webmail account
 - 1.1% of spam forged the "From:" address to appear as if sent by a legitimate webmail account – social engineering.
 - 88.2% of spam sent by botnets, falling to 77% at the end of 2010, due to declined functioning of botnets such as Grum, Mega-D, Storm, Lethic and Asprox and closure of Spamit
 - The largest botnets (Rustock, Grum, Cutwail, Maazben) send mostly pharmaceutical spam
 - over 72% of spam is less than 5kByte in size
 - 91.1% of spam contained some kind of URL

- 1.51% (1 of 66.1) of spam containing URL, exploited short URL providers
- email-borne malware of 2010
 - Stuxnet trojan – impact industrial control systems hardware
 - Targeted attacks, a.k.a. Advanced Persistent Threats – 60 attacks per day
 - Here You Have” virus (a.k.a.W32.IMSOLK.B@mm) – used old mass-mailer techniques
 - PDF Zero-day Targeted Attack
- New sites with malware blocked: 3,066 per day
- File Types in Web Hosted Malware: 26% .zip and web page file types, 19% .js and 8% .jpg
- Of all malicious blocks, 4% is spyware and 96% malware
- 22% of young domains needed 7 days to remove the threat from their legitimate site
- 6.9% of old domains needed 7 days to remove the threat from their legitimate site

Kaspersky’s security bulletin for 2010 on spam showed that:

- Global spam rate: 82.2%
- Global phish rate:0.35%
- Global malware rate: 2.2%
- command centers of the Waledac, Pushdo / Cutwail, Lethic and Bredolab botnets were closed down
- SpamIt partner program went out of business
- Bredolab botnet was used both for pharmaceutical spam and malware distribution

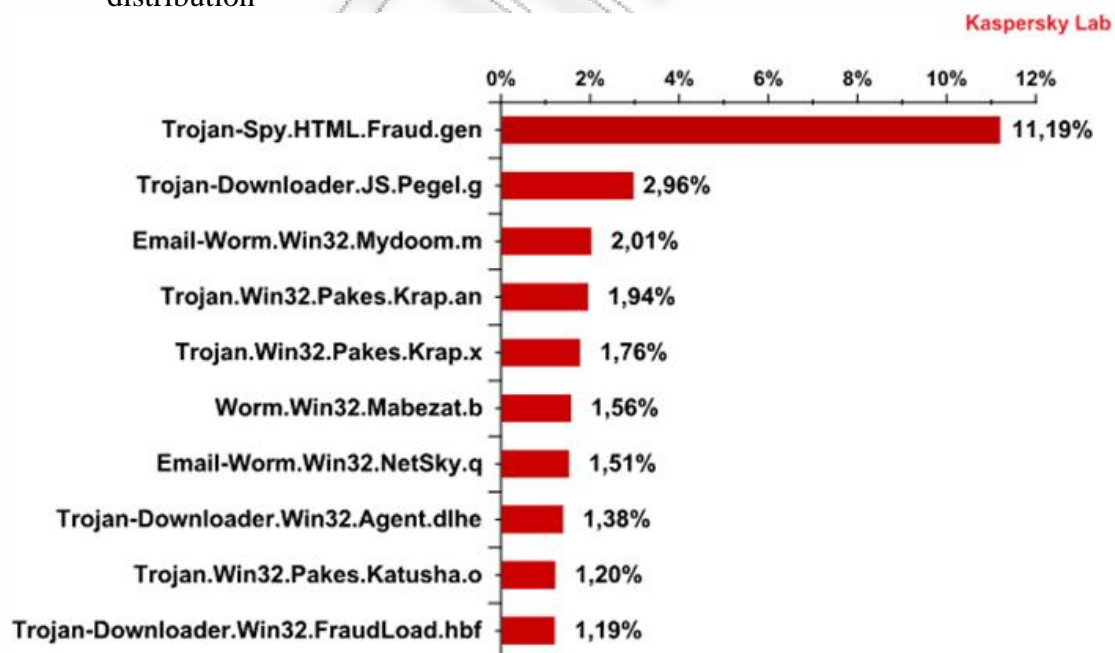


Figure 12.2.6: The Top 10 malicious programs distributed via mail traffic in 2010 [5].

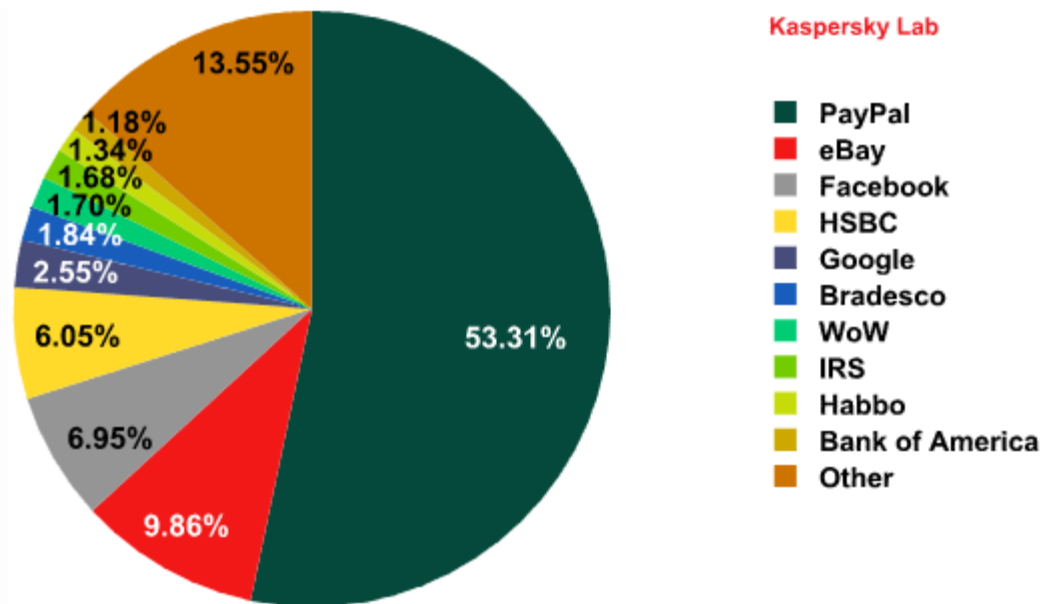


Figure 12.2.7: Top 10 organizations targeted by phishing attacks in 2010 [6]

Kaspersky's report on malware evolution for 2010 states that [37]

- Increased number of attacks on p2p networks
- estimated total number of attacks: 10 million per month on p2p networks
- Mariposa, ZeuS, Bredolab, TDSS, Koobface, Sinowal and Black Energy 2.0 botnets propagated through email, social and p2p networks
- Decreasing numbers of Rogue Antiviruses
- Trojan-SMS.AndroidOS.FakePlayer - the first real example of Android malware
- Aurora - affected large companies globally aiming at cyber-espionage and confidential commercial data theft – exploited Internet Explorer's vulnerability in remote code execution
- Stuxnet - target programmable logic controllers, potentially inflicting significant physical damage
- Stuxnet was signed by Realtec Semiconductors and JMicon.
 - These digital certificates may have been
 - Illicitly purchased by insiders
 - Stolen by using malware such as backdoors
 - Zbot or ZeuS may be capable of stealing digital certificates
- Trojans downloaded by social networks, drive-by downloads and peer-to-peer networks blocked the victim machine's operating system or Internet access and demanded that the user send an SMS message to a premium-rate number in order to receive an 'unblock code'.
- Trojans encrypt data using RSA and AES, demanding payments for restoring the data
- new type of attack appeared on Facebook in May - 'Likejacking'
- p2p networks rank second place in malware distribution, while first place rank drive-by downloads
- Number of attacks increased from 73.619.767 in 2009 to 580.371.937 in 2010

- This happened due to availability of exploit kits and self-propagating web infections
- Number of network attacks blocked by IDS increased from 219.899.678 in 2009 to 1.311.156.130 in 2010

McAfee Labs presented the following figures.

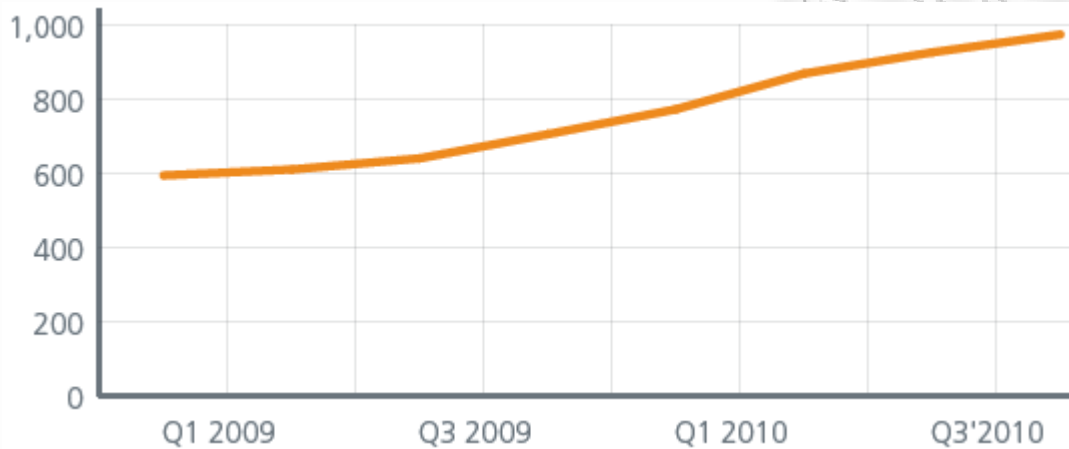


Figure 12.2.8: Mobile Malware Growth by Quarter

The figure above shows a steady growth on mobile malware. It increased 46% compared to 2009.

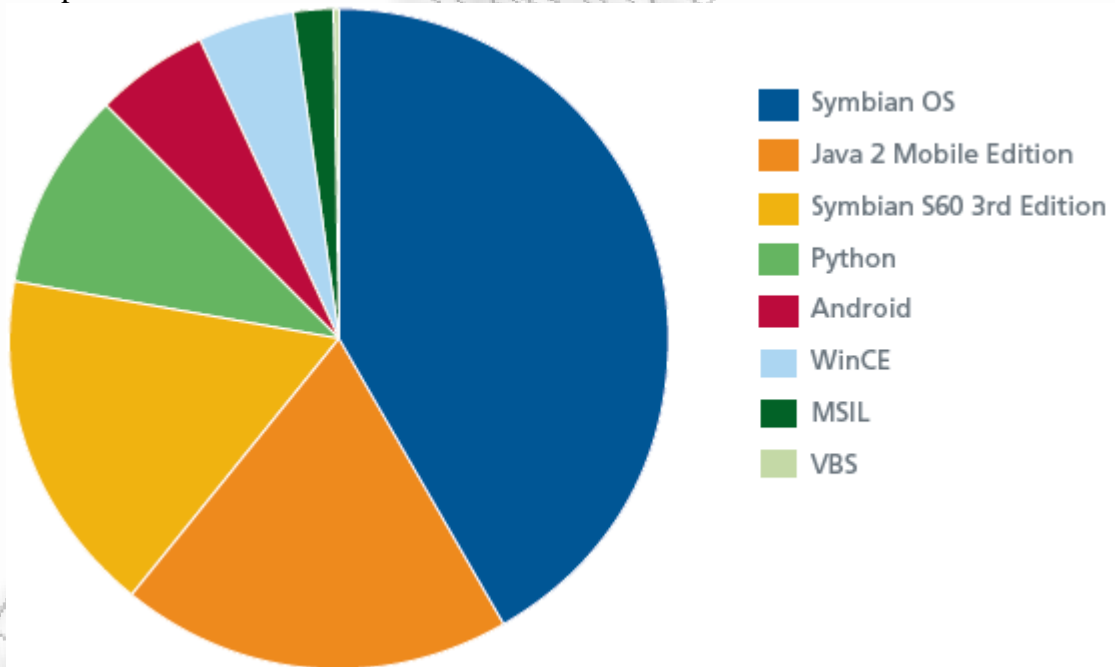


Figure 12.2.9: Mobile Threats per platform, 2009-2010

The figure above indicates that Symbian OS is the most popular platform for mobile malware developers. McAfee Labs has found 188 new threats the last 2 years and 668 since 2004.

- Global spam rate is reported to 80%.



Figure 12.2.10: The top 100 poisoned search terms for the last quarter of 2010

McAfee Labs found out that:

- 51 percent of the daily top search terms led to malicious sites
- each of these poisoned-results pages contained more than five malicious links
- almost 5 percent had a malicious link in the top 10 results alone

McAfee Labs counted 214,992 pieces of malware exploiting vulnerabilities in Adobe Acrobat and Reader. In contrast, only 2,227 malware exploited vulnerabilities detected in Microsoft Office products.

- “Crimeware” license kits to create botnets such as Blackhole v1.0.0 beta, Phoenix v2.4, Eleonore v1.6 and v1.6.2 cost from \$1500 to \$2000 annually.

From the above evidence, malware extends its propagation on various operating systems and mobile devices. Botnets, such as Zeus, are installed on both mobile phones and computers. Their main objective is to capture transaction authentication numbers from banks. Botnets were mostly responsible for spam. Almost 85% of incoming email was spam. A small percent of malware is propagated through spam, almost 1,275% and phishing attempts 0,285% Botnets are propagated through p2p. The shutting down of the McColo internet service provider resulted in the decline of spam. This is because it hosted botnet programs, such as Rustock and Cutwail, which sended spam. Drive – by downloads is the most famous way to propagate malware, followed by p2p. Malware targets not only individuals, but organizations as well. The four most targeted organizations are PayPal, e-bay, facebook and HSBC.

12.3. Malware statistics in p2p

Apart from the above findings and to the author's knowledge, no recent specific statistics were found for the amount of malware being trafficked through p2p networks. The following information derives from three previous publications made on the topic for malware in p2p.

Gryaznov's detection [5] was based on monitoring files hosted on Gnutella in 2005 and reporting malicious behavior at McAfee AVERT. It is not mentioned how the data were acquired or other parameters were involved, such as how many files were gathered, the size of files and what was queried. The following figure lists types of malware found by Gryaznov.

The top ten malware detections in P2P (Gnutella) in 2005	
Downloader-TS	7,540
W32/Tibick!p2p	1,764
W32/Generic.d!p2p	1,597
W32/Sndc.worm!p2p	1,438
VBS/Gedza	1,029
W32/Bagle.aa@MM	784
Exploit-MS04-028	757
W32/Pate.b	649
W32/Sdbot.Worm.gen	566
W32/Bagle.n@MM	535

Kalafut A. et al. [6] searched in Limewire and OpenFT. Their parameters were:

- Download only archival, executable and Microsoft Office file formats because of the severe damage they can cause.
- Scan downloaded files with ClamAV open source malware scanning software.
- Avoid searching malware in media files because malware contained in media files rely on buffer overflow type of attacks in the playback code of specific applications to do damage.
- Disable upload to avoid hosting malware.
- Remember queries sent.
- Periodic reconnection to Limewire (after 12 hours) and OpenFT (after 2 days) to observe diverse p2p views in every connection.
- Download files that Limewire considers program files: *ace, arj, awk, bin, bz2, cab, csh, cue, deb, dmg, exe, gz, gzip, hqx, iso, jar, jnlp, lzh, lha, mdb, msi, msp, nrg, pl, rar, rpm, sh, shar, sit, tar, taz, tgz, z, zip, zoo, 7z*.
- Download Microsoft Office files: *doc, ppt, and xls*.
- Do not download and scan a file with an identical name and size with a previously scanned file.
 - Re-download of clean and infected files did not change the overall conclusion
 - Malware may be polymorphic – alter file size
 - Exception on Limewire – signature might be absent. If less than 7 days have passed, wait for another 7 days before download.

The chosen file types accounted for 7.5% of all responses in Limewire and 1.3% of all responses in OpenFT.

	Limewire	OpenFT
Data collection days	45	37
Start date	4/1/06	4/9/06
Number of queries	34,268,803	12,347,509
Number of responses	32,788,921	30,538,152
Qualifying responses	2,468,327	381,851
Attempted downloads	228,722	22,231
Successful downloads	78,004	17,758
Unique clients	383,601	14,432

Figure 12.3.1: Aggregated Statistics.

In the above figure, qualifying responses are the responses which are considered to be downloaded. Attempted downloads differ from successful downloads because the host was unavailable.

They successfully downloaded 78004 files in Limewire and 17758 files in OpenFT for a period of 45 and 35 days each. In Limewire, 95 distinct malware types were found. In OpenFT, 38 malware data types were found. In Limewire, 68% of detected files contained malware while in OpenFT, 3% was the amount of detected malware. Most malware is detected exist in zip and exe files. The most popular malware is the same across Limewire and OpenFT. In each system, 5 malware are common among the top ten malware searches. The top three malware accounts for 98.5% of all malicious software in Limewire, while in OpeFT, it accounts for 75%. Queries containing movie names retrieved the most malware, while no such behavior was observed in OpenFT.

Malware hosting in Limewire by private address ranges account for 28% of all malicious responses. In OpenFT, 67% of all the malicious responses is served by one host. Limewire has a detection system that detected 6% of malware, with a 17% false positive rate.

Function	Limewire	OpenFT
Downloader	45.16%	34.78%
Worm	40.32%	39.13%
Unknown	30.65%	30.43%
Backdoor	25.81%	17.39%
Adware	4.84%	8.70%
Dialer	4.84%	4.35%
Keylogger	3.23%	0.0%

Figure 12.3.2: Function and malware percentage in Limewire and OpenFT

The above figure shows different functionalities of detected malware. The categorization is based on information provided by Kaspersky, Sophos, Symantec and the Computer associates virus information center. The percentages adding up do not give 100% because some malware contained more functionalities than one.

Berns D.A. and Eunjin J. [7] searched BitTorrent for malware. Precautions taken were:

- All file downloading and scanning on VMWare server
- Operating System: Ubuntu Linux
- ClamAV

Torrents were downloaded by BushTorrent, isoHunt, Mininova and BTJunkie. Twice a day, a torrent index site was selected and viewed all torrents under the “Application category. The download took nine days downloading 379 files, with files sizing at most ten megabytes. Their scanning with ClamAV revealed 75 files from 70 downloads infected, meaning that 18.5% of all downloads were infected by malware.

Malware Name	Number of Infected Files	Percent of Malware (Rounded)
Trojan.Small-5335	22	29.3%
Trojan.Zlob-3743	8	10.7%
Trojan.Dropper-3074	5	6.7%
Trojan.Agent-19483	5	6.7%
W32.Parite.B	4	5.3%
Trojan.Vundo-2185	3	4%
Trojan.Agent-11765	3	4%
Trojan.Spy-4973	3	4%
Trojan.Zlob-2789	2	2.7%
Trojan.Downloader-25772	2	2.7%
Trojan.Vundo-2505	2	2.7%
Others (only 1 occurrence found)	16	21.3%
Total	75	100%

Figure 12.3.3: Malware Occurrences in Sample

The above table shows the count of malware found. Fifteen infected downloads claimed to be an activation utility or key generator. Six claimed to be popular p2p file sharing applications. Five files claimed to be CD - DVD program burners. The researchers also found out that the rate of seeders of malicious downloads falls quicker than the seeders of healthy files. The authors found out that the number of seeders may be falls, as a malicious uploader may use a program, such as btrack. By modifying a line of code in the program, the malicious uploader may give any number of seeders, fooling the user to believe that, for example, 300 users are seeding the file.

13. Searching for malware in IsoHunt

Taking into consideration the above security precautions, the author has searched for malware that can be downloaded using BitTorrent. The chosen site for downloading torrents was isoHunt. On a virtual machine, an antivirus and firewall solution was installed. A scanner utilizing antivirus engines for malware detection was used.

Torrents were downloaded on the virtual machine. The files were scanned by both the antivirus solution and the online scanner. Afterwards, the torrents were downloaded using BitTorrent. The files were scanned again by both the antivirus solution and the online scanner, detecting malware. The precautions taken specifically were:

- VMware player 3.1.4
- Guest OS: Windows 7 x64
- Kaspersky Internet Security 2011 (antivirus and firewall)
- VirusTotal Uploader 2.0

IsoHunt is a BitTorrent search engine. According to IsoHunt's site on 18/06/2011, (www.isohunt.com), there are 7,342,659 torrents active, 176.15 million files, all of which size up at 12,797.82 TB and 27.30 million peers exist. A user can search IsoHunt by:

- Typing words
- Category (search by popularity or last day only)
 - All
 - Video/Movies
 - TV
 - Audio
 - Music Video
 - Games
 - Applications
 - Pictures
 - Anime
 - Comics
 - Books
 - Misc
 - Unclassified
 - Creative Commons
 - Public Domain
- Browse 60 latest torrents
- Zeitgeist of last day's most searched phrases (popular search phrases).

Search results can be limited by 1 day, 7 days, 6 months or none. The information columns for each torrent are Category, Age of torrent, Torrent Tags, Name, Size, Seeds and Leechers. The results can be sorted in order of each column, when the column title is pressed. Every torrent can be assigned a rating and comments. The rating is additive and can be positive or negative.

A registered user can do one of the following, considering reputation ratings:

- Flag a torrent file as (in which case it gets a negative rating)
 - Fake
 - Spam/Malware
 - Passworded
 - Misnamed

- Bad Quality
- Add +1 to the torrent's ratings

To the author's knowledge, rankings are added up giving a positive or negative value. In addition, the color scheme of the rated number and the comment becomes red when the ranking value is negative. If a rating has a plus, then the color becomes green.

A registered user may post a comment for the specific torrent. The comment itself may take a rating by other registered users, incrementing by +1 or decreasing by -1. BitTorrent's policy forbids users making various identities so as to avoid Sybil attacks. These +1 or -1 ratings are summed up and form the reputation of the registered user. A registered user can see which users have voted whom and how many times.

You ran out of votes.

What's your vote on user **GriM_RiPPeR**?

- Positive (+1)
- Negative (-1)
- Reset (0)

Users **GriM_RiPPeR** voted on:

- pixelz3n (1)
- cousinsven (1)
- Shorehamstreetskin (1)
- Satch_____ (-1)
- Istolealofofbread (1)
- Devils_108 (1)
- Aamon (1)
- gman28 (1)
- UndernetJunkie (1)
- deja_vu_zain (1)
- necromonger (1)
- eldestFLeTch (1)
- already_dead (1)
- fakehater (1)
- Souldragun (1)
- udipanda (1)
- Grim333 (1)
- joedles (1)
- venomuk (1)
- ftemple (1)
- djdezzie (1)
- RaceAce_UK (1)
- Septala (1)
- reverbaby01 (1)
- vymish (1)
- Telcontar1014 (1)
- CrazyMcCool (1)
- SoDaSeeD (1)
- priest31 (1)
- BouncinBunny (1)
- backfromdegrave (1)
- 1337Cyndic@ (1)
- jedijoe24 (1)
- Blood-Rain (1)
- Ozperson (1)
- smythebates (1)
- Lifechanger (1)
- defcomexperiment (1)
- BMM (1)
- IH (1)
- vjw757 (1)

Users who voted on **GriM_RiPPeR**:

- Mr Pink (1)
- AmeliaMcc30 (1)
- Shorehamstreetskin (1)
- Istolealofofbread (1)
- deja_vu_zain (1)
- UndernetJunkie (1)
- Grim333 (1)
- fakehater (1)
- romelodow123 (1)
- venomuk (1)
- Souldragun (1)
- vymish (1)
- SoDaSeeD (1)
- jedijoe24 (1)
- MonroeGas (1)
- Faroese (1)
- Ozperson (1)
- Lifechanger (1)
- smythebates (1)

[Close]

Figure 13.1: Making a registered user's reputation.

The above picture is an example of the above rating system mentioned. Registered user named GriM_RiPPeR, on June 18, Saturday, 2011, had 20 reputation points.

Adding the votes of users who voted on GriM_RiPPeR is 19. The +1 vote is by default GriM_RiPPeR's

13.1. Malware found in isoHunt

In order to try to find malware and put the personal computer at low risk, the author considered the following characteristics in isoHunt:

- Number of Seeds and Lechers (zero or not)
- Negative and Positive Ratings
- File sizes up to 20 Mbytes (due to virus total upload limitation to 20 Mbytes.)
- Filtered by selecting applications

The first application torrent downloaded was named *Roboform2Go*. According to the company producing Roboform2Go, Siber Systems (www.roboform.com/download), Roboform2Go is an application for storing contacts, bookmarks and passwords encrypted in AES, in USB sticks, so as to use them on any pc without leaving personal information. The current version for windows platforms is 7.3.2 and its size is 8.3Mbytes. When downloaded and scanned with virus total, no malicious incidents were reported.

The torrent claimed to have version 7.2.8, number of seeds 366 and number of leechers 75. It is available since 10 weeks and 6 days. It had a negative rating and a comment from a user to warn other users to not download it. When scanned by Kaspersky antivirus, it defined it as a type of trojan (Trojan.Win32.Sefnit.oiy). Uploading the file in Virustotal, 11 out of 42 security vendors (26.2%) have identified it as trojan. McAfee discovered this type on 06/06/2011. In [38], McAfee writes that this type infects win32 platforms. It adds files to the system, then writes and removes files to the disk, creates and changes registry elements of HKEY_CURRENT_USER\SOFTWARE so as to run a file. Last, it tries to make a network connection.

BugBopper [39], gives information about the identity of the malware.

Category: Trojan

Platform: Win32

Family: Sefnit

Sequence: OIY 10538 different variants of Sefnit have existed and this is a very early variant.

Threat to Privacy: High

Threat to Productivity: Moderate

Threat to System Integrity: High

Overall Risk: High

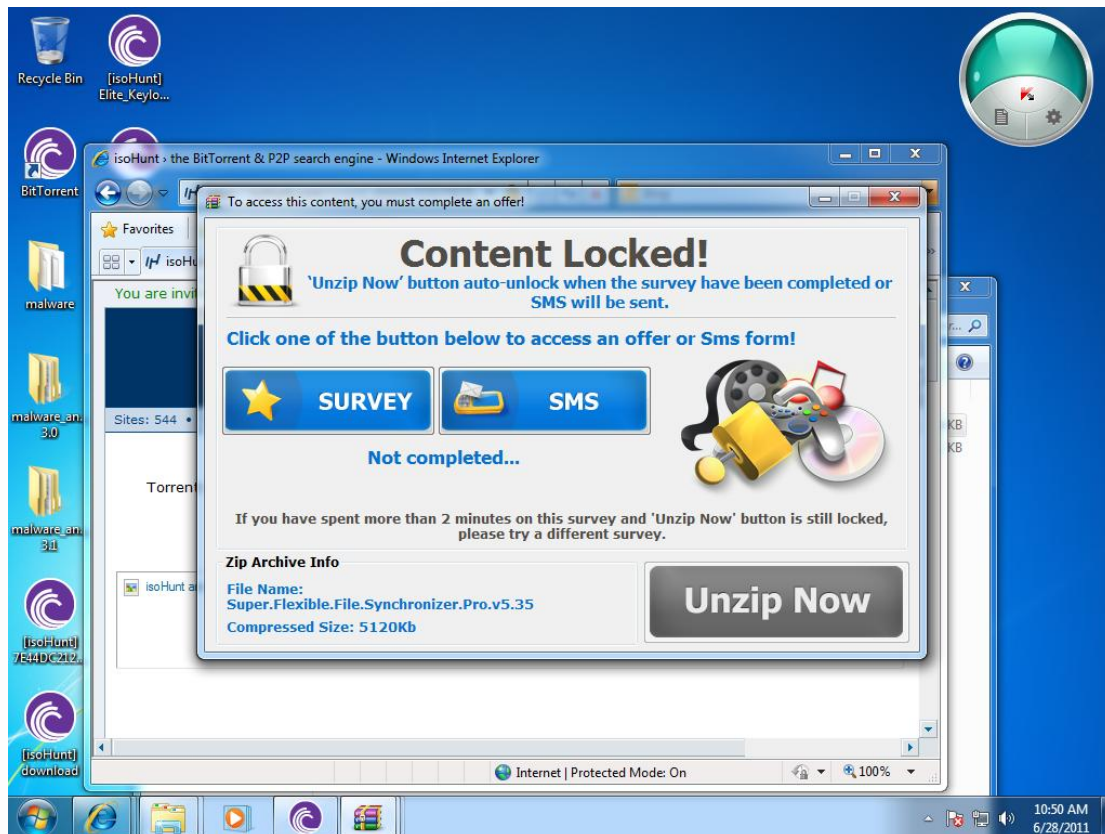
Babylon Pro v8.1.0.r16 is the previous version of Babylon Pro v9, a translation program. The torrent had negative rating, one comment to avert people from downloading the file, 10.63Mbytes, 366 seeds and 62 leechers. Kaspersky antivirus identified it as a trojan downloader (Trojan-Downloader.NSIS.Murlo.i). Uploading

the file on Virustotal showed that 28/42 (66.7%) recognized it as a trojan. Microsoft sorts it in the W32/Alureon family [40]. This family type of trojans is data stealers. The attackers intercept incoming and outgoing internet traffic to gain confidential information, such as user names, passwords and credit card data. It may allow the attacker to transmit malicious data to the infected computer. The trojan may modify DNS settings on the infected computer (by altering registry values and subkeys) so the attacker may perform the above tasks. Various instances of this family exist.

Another malware found was one named *Microsoft Office 2010.rar*. It has been on for 10.2 hours, its size is 7.12Mbytes, 633 seeds and 127 leechers. It has a negative rating and a warning comment. The file revealed to be a trojan (Trojan.W32.VBKrypt.djsf). Kaspersky detected it on June 14 2011. VBKrypt is a family of Visual Basic compiled threats, usually encrypted or compressed [41].

The same trojan type occurred (Trojan.W32.VBKrypt.djsf) when the torrent named *PERMANENTLY ACTIVATE OFFICE 2010 PROFESSIONAL PLUS.rar* was downloaded. This file was 1.6 days old, 93.09Kbytes size with 5256 seeders and 7859 leechers.

A different torrent named *YouTube Downloader* was revealed to redirect to a phishing site: hxxp://cmpx.mt-50.com/1897/119?aid=cd4462&pid=1438&sid=&bid=17036. The files the torrent downloaded were not named YouTube downloader but *Super.Flexible.File.Synchronizer.Pro.v5.35 CRACKED.zip*. It had a negative rating score, one comment saying it was password protected, 4.44Mbytes, 359 seeders and 71 leechers. When the file was downloaded, it was 5.29Mbytes. The icon posed as a .rar icon but it was in fact a .exe. When executed the following window was opened:



When the button SURVEY was pressed, it opened isoHunt with the following URL:

https://isohunt.com/torrent_details/315175829/?tab=summary

The torrent to download was not available. Task manager revealed that five connections to a remote server were stopped. Kaspersky denied access on the site as it identified it as phishing. When the file was uploaded on VirusTotal, no vendor said it was malware.

An application downloaded that was not a trojan was a Windows Elite Keylogger 4.9. The reason mentioning it here is because although it reported not having any seeds or leechers, when added on BitTorrent, 6 seeds and 24 leechers appeared. When uploaded on VirusTotal, 18/42 (49%) identify it as a Keylogger and not as malware.

A torrent claiming to have 5683 seeders and 51 leechers, but when trying to download it, no seeders or leechers were present, was turbowire-2.5.exe.

14. Comparing findings with previous research

The above trojans detected are few of the many trojan types and families detected by previous researchers. The VMware player and Kaspersky Internet Security have played a vital role in contaminating the malware and preventing it from infecting the host machine. When each file was downloaded, VirusTotal scanned it, proving that not every antivirus vendor has created a signature for their databases. Moreover, the percent of detection has never reached 100%, meaning that heuristic detection is needed to detect threats not recognized yet. Furthermore, no antivirus solution can detect 100% of all threats. Its best to take precautions than no precautions at all.

The relationship between the suspicious file and the comments made for it, if any, on isoHunt, is relevant to the file's malicious content. Moreover, the negative ratings comply with the comments made for the malicious file. The more seeders and leechers a torrent has, does not prove necessarily that the designated file does not contain malware. An application may have been used to alter these values. The same speculation is made for the Keylogger program found. This finding reinforces the need for adopting protection on personal computers. A firewall was crucial in executing the malware content, as it prevented the malware from connecting to remote attacking hosts.

One can comment on the peer reputation on malware, as it may be susceptible to Sybil attacks. A user may vote himself on various comments made, so as to gain trust on existing users. IsoHunt's policy on this, states that if a person tries such an action, that person will be banned from isoHunt's community.

In general, if a person wishes to locate malware in search engines for p2p systems, one can look for 1) negative ratings, 2) comments and 3) misleading file sizes. Looking at the numbers of seeders and leechers in order to avoid malware may prove misleading.

15. Conclusion

The ever-growing number of malware will always alert people to take precautions. Attackers will try to propagate their malware using every available means of transporting files. Decentralized p2p is an easy way of propagating malware, as the attacker needs access on a torrent search engine, such as isoHunt and Demonoid, register anonymously and upload a file. The community of search engine users deters other users from downloading malware files by using descriptive comments and negative ratings. The capability of rating a user's comment positively or negatively may restrain users from giving false comments, because it could damage their reputation.

P2p programs are one of the most popular ways in transporting malware and pirated content as well. P2p programs should be downloaded by trusted sites and not other sites as they might contain viruses themselves. A firewall is needed to block TCP ports and program vulnerabilities should be addressed to lessen exploits from other malware. The threat level of malware is calculated by considering the damage it can cause on a computer and its distribution.

In order to create a secure environment, various elements should be considered, such as where the place of the environment, people accessing it, threats and assets to be protected. Limiting a virus in a virtual environment, running an antivirus solution and a firewall may prove one day insufficient, as malware may find a way to bypass antivirus solutions and virtual environments, thus contaminating the host machine, causing irreparable damage.

Avoiding downloading pirated content, participating in torrent search engine communities by commenting and rating torrents is a way of protecting oneself from malware in p2p. Installing a firewall, an antivirus and using passwords to protect users from entering a hazardous virtual environment are basic protection. But checking a file's size to match with the actual size and comparing its release date on the torrent search engine to the normal release date worldwide, as well as the version to be downloaded are key factors in preventing the infection before even starting the download process. As long as users think and take precautions before downloading, considering seriously the threats and the value of their assets, they can and will use p2p programs without the fear of their assets losing their confidentiality, breaking their integrity or making them unavailable to them.

16. References

- [1] Schollmeier, R., August 2001, "A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications", Institute of Communication Networks, Technische Universität München, 80333 München, Germany, Available at: <http://origin-www.computer.org/plugins/dl/pdf/proceedings/p2p/2001/1503/00/15030101.pdf?template=1&loginState=1&userData=anonymous-IP%253A%253AAddress%253A%2B79.166.69.22%252C%2B%255B140.98.196.192%252C%2B127.0.0.1%252C%2B79.166.69.22%255D>, Accessed on: 28 December 2010.
- [2] Androutsellis, T.S. and Spinellis, D., December 2004, "A Survey of Peer-to-Peer Content Distribution Technologies", Athens University of Economics and Business, Available at: <http://www.dmst.aueb.gr/dds/pubs/jrnl/2004-ACMCS-p2p/html/AS04.html>, Accessed on: 28 December 2010.
- [3] Kramer, S. and Bradfield, J.C., September 2009, "A general definition of malware", Journal in Computer Virology, Volume 6, Number 2, p. 105-114, Available at: <http://www.springerlink.com/content/x537315445477225/fulltext.pdf>, Accessed on: 29 December 2010.
- [4] The Government of the Hong Kong Special Administrative Region, February 2008, "PEER-TO-PEER NETWORK", Available at: <http://www.infosec.gov.hk/english/technical/files/peer.pdf>, Accessed on 28 December 2010.
- [5] Gryaznov, D., July 2006, "MALWARE IN POPULAR NETWORKS", McAfee AVERT, Network Associates, Inc., Beaverton, OR 97006, USA, Available at: <http://faculty.washington.edu/moishe/moscow/gryaznov.pdf>, Accessed on: 30 December 2010.
- [6] Kalafut, A. Acharya, A. and Gupta, M., September 2006, "A Study of Malware in PeertoPeer Networks", Internet Measurement Conference 2006, Rio de Janeiro, Brazil, Available at: <http://conferences.sigcomm.org/imc/2006/papers/p33-kalafut.pdf>, Accessed on: 30 December 2010.
- [7] Berns, A.D. and Jung, E.J., April 2008, "Searching for Malware in BitTorrent", University of Iowa Computer Science Technical Report UICS-08-05, Available at: <http://www.cs.uiowa.edu/~adberns/UICS-08-05.pdf>, Accessed on 30 December 2010.
- [8] P2P Foundation:, July 2007, "Gnutella - P2P Foundation:.", Available at: <http://p2pfoundation.net/Gnutella>, Accessed on: 30 December 2010, Updated on 25 January 2010
- [9] Cohen, F., 1989, "Computational Aspects of Computer Viruses", Computers & Security 8, p.325-344, The Radon Project, Pittsburgh, PA, USA, Available at:

http://www.sciencedirect.com/science?_ob=MIimg&_imagekey=B6V8G-45K52VT-2R-1&_cdi=5870&_user=3828026&_pii=0167404889900898&_origin=search&_coverDate=06%2F30%2F1989&_sk=999919995&view=c&wchp=dGLzVzz-zSkWA&md5=274be85c9036c83adde31ebdf4ee9d67&ie=/sdarticle.pdf, Accessed on: 9 January 2011

[10] Cohen, F., 1989, "A Formal Definition of Computer Worms and Some Related Results", Computers & Security 11, p.641-652, ASP, P.O. Box 81270 Pittsburgh, PA, USA, Available at: http://www.sciencedirect.com/science?_ob=MIimg&_imagekey=B6V8G-45JWSK9-38-1&_cdi=5870&_user=3828026&_pii=016740489290144G&_origin=search&_coverDate=11%2F30%2F1992&_sk=999889992&view=c&wchp=dGLzVtb-zSkWA&md5=4409259ffb32578d631b6a8f70c23cb7&ie=/sdarticle.pdf, Accessed on: 9 January 2011

[11] University at Albany-SUNY, "Glossary-Information Security", Available at: <http://www.albany.edu/its/glossary.htm>, Accessed on: 9 January 2011

[12] Securelist, "Trojans - Securelist", Available at: <https://www.securelist.com/en/threats/detect/trojan-programs?behavior=29>, Accessed on: 9 January 2011, Updated at: 30 June 2011.

[13] Securelist, "Adware - Securelist", Available at: <https://www.securelist.com/en/threats/detect/adware>, Accessed on: 9 January 2011, Updated at: 30 June 2011

[14] Securelist, "Riskware - Securelist", Available at: <https://www.securelist.com/en/threats/detect/riskware>, Accessed on: 9 January 2011, Updated at: 30 June 2011

[15] Securelist, "Glossary - Securelist", Available at: <https://www.securelist.com/en/glossary>, Accessed on: 9 January 2011, Updated at: 30 June 2011

[16] Securelist, "Software vulnerabilities - Securelist", Available at: <https://www.securelist.com/en/threats/vulnerabilities?chapter=35>, Accessed on: 9 January 2011, Updated at: 30 June 2011

[17] Securelist, "Trojan-Downloader.Win32.Small.cdk", Available at: <http://www.securelist.com/en/descriptions/142058/Trojan-Downloader.Win32.Small.cdk>, Accessed on: 3 March 2011.

[18] NsPack, "NsPack 3.7 home", Available at: <http://www.nspack.com-about.com/>, Accessed on 3 March 2011.

- [19] McAfee Labs Threat Center, “W32/Brepibot - Malware - McAfee Labs Threat Center”, Available at: <http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=133091>, Accessed on: 3 March 2011
- [20] McAfee Labs Threat Center, “Downloader-UA_h Virus Profile & Definition”, Available at: <https://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=144503>, Accessed on: 3 March 2011.
- [21] SpywareRemoval, “FBrowsingAdvisor Removal Guide”, Available at: <http://www.spywareremove.com/removeFBrowsingAdvisor.html>, Accessed on: 3 March 2011.
- [22] Securelist, “Exploit.Win32.MS04-028.gen - Securelist”, Available at: <http://www.securelist.com/en/descriptions/old57108>, Accessed on: 3 March 2011
- [23] PANDA SECURITY, “Threat Level - Malware & Virus in The World”, Available at: <http://www.pandasecurity.com/enterprise/security-info/about-malware/technical-data/date-4.htm>, Accessed on: 26 March 2011
- [24] Infocon SANS Internet Storm Center, “Cooperative Network Security Community - Internet Security”, Available at: <http://isc.sans.org/infocon.html>, Accessed on: 30 May 2011
- [25] Aycock, J. and Barker, K., “Creating a Secure Computer Virus Laboratory”, EICAR 2004 Conference CD-rom: Best Paper Proceedings, Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.58.2094&rep=rep1&type=pdf>, Accessed on: 19 March 2011.
- [26] Wen, Y. and Wang, H., November 2007, “A Secure Vital Execution Environment for Untrusted Code”, Information Security and Cryptology - ICISC 2007 10th International Conference, Seoul, Korea, Available at: <http://www.springerlink.com/content/978-3-540-76787-9/#section=368536&page=3&locus=52>, Accessed on: 19 March 2011.
- [27] Hu, J. Cordel, D. and Meinel, C., 2004 “A Virtual Laboratory for IT Security Education”, FB IV – Informatik Universitaet Trier D-54286 Trier, Germany, Available at: http://www.hpi.uni-potsdam.de/fileadmin/hpi/FG_ITS/papers/Trier-Emisa04-Hu.pdf, Accessed on: 20 March 2011.
- [28] Noël, R., “Building a Security Test Environment”. Protecting Information and Securing Your Network – SecureOps Inc., Available at: http://www.secureops.com/pdfs/wp_Richard_Noel.pdf, Accessed on: 19 March 2011.
- [29] Kaspersky Labs, 2011, “Safe Run Technology in Kaspersky Internet Security 2011”, Available at: <http://www.google.gr/url?sa=t&source=web&cd=3&ved=0CDEQFjAC&url=http%3A%2F%2Fwww.kaspersky.com%2Fview.html%3Fid%3D24&rct=j&q=sandbox%20kaspersky&ei=W8oETePbJsfIswadxe37CQ&usg=AFQjCNG1hek74KzQsae6whcaANMnoH4ygA>, Accessed on: 12 December 2011.

- [30] Lawton, G., December 2002, "Virus Wars: Fewer Attacks, New Threats", Computer, Volume 35, Issue 12, p.22-24, IEEE Xplore, Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1106172>, Accessed on 12 December 2011.
- [31] Fahimian, S. Movahed, A. and Kharrazi, M., 2010, "Passive Worm and Malware Detection in Peer-to-Peer Networks", IEEE/IFIP International Symposium on Trusted Computing and Communications (Trustcom10), Available at: <http://sina.sharif.ir/~kharrazi/pubs/trustcom10.pdf>, Accessed on: 20 March 2011.
- [32] Castelli, J., December 2001, "Choosing Your Anti-virus Software", InfoSec Reading Room, Sans Security Essentials GSEC practical assignment Version 1.3, Available at: http://www.sans.org/reading_room/whitepapers/commercial/choosing-anti-virus-software_784, Accessed on: 27 March 2011.
- [33] Envisional, January 2007, "Technical report: An Estimate of Infringing Use of the Internet", Version 1.8 Envisional Ltd, Betjeman House, 104 Hills Road, Cambridge, Available at: http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf, Accessed on: 4 May 2011
- [34] Eurostat newsrelease, February 2011, "EUROPA - Press Releases - 8 February 2011: Safer Internet Day Nearly one third of internet users in the EU27 caught a computer virus 84% of internet users use IT security software for protection" Available at: <http://europa.eu/rapid/pressReleasesAction.do?reference=STAT/11/21>, Accessed on: 20 April 2011
- [35] faqs.org, January 1998, "What is Usenet?", Available at: <http://www.faqs.org/faqs/usenet/what-is/part1/>, Accessed on: 30 December 2010
- [36] Hosted Services by Symantec, 2011, "MessageLabs Intelligence: 2010 Annual Security Report", Available at: http://www.messagelabs.com/mlireport/MessageLabsIntelligence_2010_Annual_Report_FINAL.pdf, Accessed on: 20 April 2011
- [37] Kaspersky lab, January 2011, "Malware Evolution 2010: Results and Forecasts", Available at: http://www.kaspersky.com/reading_room?chapter=207717661, Accessed on: 22 April 2011
- [38] McAfee, June 2011, "Generic.dx!ztu!1A483EC4B912", Available at: http://vil.nai.com/vil/content/v_518625.htm, Accessed on: 23 June 2011
- [39] BugBopper, January 2011, "Trojan.Win32.Sefnit.oiy", Available at: <http://www.bugbopper.com/NameLookup.asp?Name=Trojan.Win32.Sefnit.oiy>, Accessed on: 28 June 2011

[40] VirusTotal - Free Online Virus, Malware and URL Scanner, Report on File name Babylon8_setup.exe, Submission date 28 June 2011, Available at: www.virustotal.com/file-scan/report.html?id=4594b9955640667268aed5244d1e0290aad4be73dd7b2edcfa5e1321083afe56-1309263537

[41] CA technologies, June 2011, "Win32/VBKrypt.DN - CA Technologies", Available at: <http://gsa.ca.com/virusinfo/virus.aspx?id=170468>, Accessed on: 28 June 2011

[42] Schmugar, C., May 2008, "Fake MP3s Running Rampant, Blog Central", McAfee Blog Central, Available at: <http://blogs.mcafee.com/mcafee-labs/fake-mp3s-running-rampant>, Accessed on 9 March 2011

17. Figures

[1] Architecture_hybridP2P.jpg, Available at: http://one-project.sourceforge.net/wiki/images/0/0e/Architecture_hybridP2P.jpg

[2] Architecture_pureP2P.jpg, Available at: http://one-project.sourceforge.net/wiki/images/d/d9/Architecture_pureP2P.jpg

[3] PANDA SECURITY, “Threat Level - Malware & Virus in The World”, Available at: <http://www.pandasecurity.com/enterprise/security-info/about-malware/technical-data/date-4.htm>, Accessed on: 26 March 2011

[4] Infocon SANS Internet Storm Center, “Cooperative Network Security Community - Internet Security”, Available at: <http://isc.sans.org/infocon.html>, Accessed on: 30 May 2011

[5] ksb2010_spam_pic18_all.png, January 2011, Available at: http://www.securelist.com/en/images/vlill/ksb2010_spam_pic18_all.png

[6] ksb2010_spam_pic21_en.png, January 2011, Available at: http://www.securelist.com/en/images/vlill/ksb2010_spam_pic21_en.png